DEFENCE R&D DÉFENSE

DREO Secure Video Conferencing and High Speed Data Encryption Tests for Inmarsat-B Satellite Terminals (U)

James D. Lambert
Defence Research Establishment Ottawa

DEFENCE RESEARCH ESTABLISHMENT OTTAWA

TECHNICAL MEMORANDUM
DREO TM 1999-084
October 1999

National Defence Défense nationale

Canada

ABSTRACT

The aim of this report is to describe the results of a series of tests performed between 1996 and 1999 using Inmarsat-B satellite terminals. These tests were designed to evaluate the use of commercial-off-the-shelf equipment in demonstrating low-rate, secure video conferencing, multiplexed voice and data circuits, and local area network extension services via the Inmarsat-B 64 kb/s high speed data service. Successful demonstrations of both secure point-to-point, and secure remote-to-Defence Video Conferencing Network were conducted.

RESUMÉ

Ce document détaille les resultats d'une série de tests exécutés entre 1996 et 1999 utilisant des terminaux satellites Inmmarsat-B. Ces tests ont été créés pour évaluer l'utilisation d'équipements standards disponibles sur le marché dans la démonstration de communication à débit faible, de vidéoconférence sécure, des circuits multiplexés de voix et de donnés, et d'extension de services de réseau local en utilisant le service de transmission ultra-rapide de données de 64 kb/s d'Inmarsat-B. Les démonstrations de communications sécurisés de point-à-point ont été réussites ainsi que des communications sécurisés d'un point à distance au Réseau de Vidéoconférence de la Défense.

ACKNOWLEDGEMENT

The author would like to acknowledge the participation and generous support of Mr Joel Brassard from Bell Canada in the preparation and conduct of many of the experiments described in this report.

EXECUTIVE SUMMARY

In response to recent interest from DND in the use of secure video conferencing between remote units and the Defence Video Conferencing Network (DVCN), the DND Directorate of Communications and Electronics Engineering Maintenance (DCEEM) prepared an Inmarsat-B High Speed Data (HSD) Trial directive in February 1996. The purpose of the directive was to evaluate the use of 64 kb/s satellite data links in supporting low-rate secure video conferencing.

Following an initial demonstration of the Inmarsat-B High Speed Data service by Bell Canada and TD Communications Ltd. in March 1996, DREO participated in a second series of secure data trials jointly supported by Bell Canada, TD Communications, the Communications Security Establishment (CSE) and Teleglobe Canada. This report will document the results of the secure data trials, and some additional follow-on demonstrations conducted at the request of DND.

The experiments described in this report were conducted over the period from July 1996 to April 1999, and included three phases. The first phase consisted of trials were conducted in mid-1996 to characterize the performance of individual pieces of Commercial Off The Shelf (COTS) equipment. The resulting performance data was used to integrate the baseband video equipment, the encryption devices, the Inmarsat-B terminals and the Integrated Services Digital Network (ISDN) terminal into a reliable end-to-end HSD data link.

The second phase was focussed on conducting an actual live demonstration of a secure video conference link with the DVCN network. This trial required a solution to the problem of connecting an encrypted 64 kb/s video conference feed with the secure 384 kb/s DVCN network. It was successfully concluded with a live demonstration at the DVCN Control Center in Ottawa in late 1996.

The third phase of this project was to demonstrate secure data transfers over the Inmarsat HSD service, and to verify crypto compatibility between the older KG-84C and the newer KIV-7 encryption devices. After some delays due to other priorities, this goal was completed in 1999 with a demonstration of secure TCP/IP Local Area Network extension services.

Lambert, James D., DREO Secure Video Conferencing and High Speed Data Encryption Tests for Inmarsat-B Satellite Terminals. Defence Research Establishment Ottawa, DREO TM 1999-084, October 1999.

SOMMAIRE

Afin de répondre à l'intérêt démontré par le MDN envers la vidéoconférence protégée entre unités distantes et le Réseau de vidéoconférence de la Défense (RVD), la Direction Génie et maintenance (communications et électronique) du MDN a préparé une directive d'essai de transmission de données haute vitesse par Inmarsat-B en février 1996. Cette directive avait pour but l'évaluation de l'utilisation de liaisons de données à 56 kbit/s par satellite pour la réalisation de vidéoconférences protégées à faible débit.

Suite à une démonstration initiale du service de données haute vitesse Inmarsat-B par Bell Canada et TD Communications ltée, en mars 1996, le CRDO a participé à une seconde série d'essais de transmissions protégées réalisées à l'aide de Bell Canada, TD Communications, le Centre de sécurité des télécommunications (CST) et Téléglobe Canada. Le présent rapport documente les résultats des essais de transmissions protégées ainsi que certaines démonstrations consécutives réalisées à la demande du MDN.

Les expériences décrites dans ce rapport ont eu lieu pendant la période de juillet 1996 à avril 1999 et elles se répartissaient en trois phases. La première se composait d'essais réalisés au milieu de 1996 et qui visaient à caractériser les performances d'équipements individuels disponibles sur le marché commercial. Les données de performance résultantes ont été utilisées afin d'intégrer l'équipement vidéo en bande de base, les dispositifs de cryptage, les terminaux Inmarsat-B et le terminal de réseau numérique à intégration de services (RNIS) à une liaison de données HSD fiable de bout en bout.

La deuxième phase était axée sur la réalisation d'une démonstration en direct d'une liaison de vidéoconférence protégée avec le réseau RVD. La principale difficulté de cet essai était de relier une source de vidéoconférence à 64 kbit/s avec le réseau RVD protégé à 384 kbit/s. Cet essai s'est conclu avec succès par une démonstration en direct au Centre de contrôle du RVD, à Ottawa, à la fin de 1996.

La troisième phase de ce projet consistait à faire la démonstration de transferts de données protégés au moyen du service HSD d'Inmarsat-B et de vérifier les compatibilités cryptographiques entre l'appareil cryptographique KG-84C, plus ancien, et le KIV-7, plus récent. Après certains retards causés par d'autres priorités, cet objectif a été atteint en 1999, avec une démonstration de services d'extension TCP/IP protégés de réseaux locaux.

Lambert, James D., Essais de transmission de vidéoconférence protégée et de données cryptographiques haute vitesse pour les terminaux du satellite Inmarsat-B. Centre de Rechereches pour la Défense Ottawa, DREO TM 1999-084, October 1999. (en anglais)

TABLE OF CONTENTS

TABLE OF CONTENTS - continued

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Recent DND interest has been expressed in low-rate secure digital video conferencing from deployed mobile units via satellite to the existing Defence Video Conferencing Network (DVCN). This has led in part to the establishment of an Inmarsat-B terminal test-bed facility at DREO, with the objective of providing test facilities for evaluating possible equipment configurations for use by DND and other interested government agencies.

A previous series of tests was conducted by DND/DCEEM, Bell Canada and TD Communications Inc. in February/March 1996 in accordance with the Inmarsat-B High Speed Data (HSD) Trial Directive prepared by the Directorate of Communications and Electronics Engineering Maintenance (DCEEM). These tests are documented in [1], and demonstrated the use of an Inmarsat-B portable satellite terminal to establish a 64kB data link via an Inmarsat Earth Station into the existing Integrated Services Digital Network (ISDN) ([2], pp1747-1776). The demonstration links carried either multiplexed DND voice and data circuits, or a 64 kB point-to-point video conference link. Due to administrative problems, authority could not be obtained to employ DND cryptographic equipment, hence the trial was limited to demonstrating non-secure circuits only.

This report will document the results of a second series of tests performed in late 1996 as a partnership effort by several agencies. These tests were intended specifically to demonstrate the use of commercial off-the-shelf (COTS) equipment in the implementation of 64 and 128 kb/s **secure** digital video and multiplexed data links from highly portable satellite terminals. Agencies contributing equipment, technical or financial support to the test program include the Bell Canada DND Engineering Group, the Communications Security Establishment (CSE), the Defence Research Establishment Ottawa (DREO), and Teleglobe Canada.

2. EQUIPMENT CHARACTERIZATION

The following equipment was obtained for the test program:

Item	Qty	Manufacturer	Model	Description
1	2	MobileSat	Inmarsat-B Lynxx	Satellite Terminals with remote antenna kits
2	2	MobileSat	VideoLynxx	Digital video conferencing units
3	4	Allied Signal	KIV-7	Data encryption units
4	2	RAD	IMX-6L	Inverse multiplexers
5	1	Adtran	ISU2x64	ISDN terminal adapter
6	2	PCSI	CS8000 TDM	Voice/data multiplexers
7	2	TTC	FireBerd 6000	Serial data analyzers

Initial tests with this equipment revealed a number of interconnection problems which required a complete characterization of the RS-449 and RS-530 serial data interfaces offered by each type of equipment. Some of the most significant interfacing problems are discussed in this section, and a series of tables is presented summarizing the performance of each unit.

2.1 Inmarsat B Lynxx Terminal

The Inmarsat B Lynxx terminal is a highly portable satellite terminal which provides a single voice, fax or high speed data circuit from any location in the world between 70 deg. north and 70 deg. south latitudes, using the global Inmarsat B satellite service. The operation of the terminal is covered in the user manual [3], but some critical HSD interface issues had to be resolved for the applications discussed in this report. The terminal was configured to operate as an RS-422/449 Data Communications Equipment (DCE) device ([2] pp1530-1541), with Transmit Timing (TT) provided by the DCE. All signals are accessible via a standard DB37F connector. Transmit and receive clock and data signals follow the RS-449 standard, but the secondary, or handshake signals do not. Table 1 summarizes the operation of the signalling at the RS-449 connector on the Inmarsat B Lynxx Terminal. Of all the normal modem handshake signals, only Receiver Ready (RR) is provided by the terminal, and only when a valid HSD circuit exists. This necessitates non-standard cabling to any Data Terminal Equipment (DTE) device which requires Data Mode (DM) or Clear to Send (CTS) signals from the DCE.

The availability of an Inmarsat HSD data loopback call was explained by personnel at the Teleglobe operations center, and this feature was used extensively to confirm equipment performance during these trials. The most basic test used to confirm proper operation of the Inmarsat B terminal was to connect a Fireberd data analyzer to the RS-449 HSD port, and place an HSD data loopback call through the Teleglobe earth station. A good connection would result in essentially error-free communications at 64 kb/s, but occasional links were obtained which provided very marginal performance. Some drop-outs of the data link were also observed, accompanied by error messages on the terminal master handset. Two different Inmarsat-B terminals were tested in this manner, and there was some indication that one of the terminals was experiencing intermittent hardware problems. These were not severe enough to interfere with the planned tests, but were noted for eventual warranty repair action.

Some experiments were done to determine whether two of the Inmarsat-B terminals could share one common antenna. The intent was to show the feasibility of minimizing the amount of size and weight which would be required on a stabilized antenna platform mounted on a ship. Figure 1 is a diagram of the radio frequency (RF) combiner circuit which was provided by TD Communications Inc. for this test. The most noticeable limitation of this method is that each terminal experiences a minimum of 3 dB loss in transmit power due to cabling and insertion losses through the transmit power combiner circuit. A preferred method would be to use this circuit at a lower powered intermediate frequency (IF), and include a linear up-converter and power amplifier on the combined signal before routing to the common antenna. Testing of the two terminals using the combiner circuit and common antenna was done with HSD data loopback calls, and simultaneous operation of each 64 kb/s data link was confirmed. There was an increased tendency to encounter unreliable links when both HSD calls were in operation, and this was attributed in part to possible mutual interference effects in the power combiner, and more marginal uplinks due to the 3 dB loss in transmit power through the combiner circuit.

2.2 ADTRAN ISU 2x64 ISDN Terminal Adapter

An essential component of all tests described in this report is the use of ISDN data circuits to complete the link from the Inmarsat earth station to the intended destination of the data call. As part of each Inmarsat-B terminal registration, Teleglobe Canada reserves two ISDN phone numbers which are dedicated to the HSD service for the terminal. Users of the HSD service require as a minimum one ISDN Microlink connection, which is referred to as "2B+D", meaning two 64kb/s Bearer channels and one 16 kb/s Signalling channel. Again, two ISDN phone numbers are assigned to each Microlink, so the two Bearer channels can be used independently if required. The ISDN Microlink service requires user provided Terminal Adapter equipment to make the two 64 kb/s channels available to the user. For this project, the Terminal Adapter (TA) selected was an ADTRAN ISU 2x64, which is capable of offering independent use of each 64 kb/s bearer channel, or of applying a standard BONDING1 protocol to provide a composite 128 kb/s data circuit.

Table 2 summarizes the setup parameters used for the ADTRAN TA during these tests. The DCE interface on the TA was standard RS-530 signalling, with Transmit Timing (TT) provided by the TA. As indicated in section 2.3 below, the Clear to Send (CS) handshake line was configured to "Forced On" for compatibility with the KIV-7 encryption unit. Initial testing of the ISDN connection was done by attaching Fireberd analyzers to both channel one and two of the ADTRAN TA, then placing a 64 kb/s data call from one ADTRAN port to the second one. Initial bit error readings were observed during these tests, but were subsequently traced to an ISDN circuit problem. This was corrected with a trouble call to the circuit provider. With the problem resolved, further testing indicated the ISDN Microlink service to be error-free and stable. The availability of an ISDN data loopback call was explained by personnel at the BELL ISDN operations center, and this feature was used extensively to confirm equipment performance during these tests.

2.3 KIV-7 Comsec Module

The KIV-7 encryption device was extensively tested in this project as the means to provide a secure mode for Inmarsat B HSD video conferencing and multiplex data circuits. In all cases, the KIV-7 was inserted in the synchronous RS-449 data link between a DCE device such as the Inmarsat B SATCOM terminal, and a DTE device such as the VideoLynxx video conferencing terminal. Operation of the KIV-7 is described in it's user guide [5], but

additional information on the use of various configuration parameters was obtained directly from both DND/CSE and the manufacturer, Allied Signal Inc. Table 3 summarizes the configuration settings used for these tests.

Initial tests with the KIV-7 were done using the configuration shown in Figure 2. The communications circuit was provided by an ADTRAN dual 2x64 ISDN terminal adapter (TA) [6] providing two RS-530 synchronous interfaces. Table 2 summarizes the configuration settings of the terminal adapter. The data terminal devices at each end of the link were Fireberd 6000 Data Error Analyzers, equipped with RS-449 interface plug-ins. Adapter cables were used to convert from DB25 RS-530 connectors to DB37 non-RS-449 connectors on the KIV-7 black side, and from DB37 RS-449 connectors to DB37 non-RS-449 connectors on the KIV-7 red side. Tests were performed by placing 64 kb/s data calls from one port of the terminal adapter to the second. When the ISDN circuit was established, crypto synchronization of the two KIV-7 was performed, and the resulting data link evaluated with the data analyzers.

Results of these initial tests indicated that the KIV-7 would automatically achieve crypto sync in several different modes (RED, NR, OP2) after an ISDN data link was established. Initial bit error readings were traced to an ISDN circuit problem which was corrected with a trouble call to the circuit provider. Subsequent tests indicated reliable, consistent encrypted communications with no measurable bit error. The only problem found in using the KIV-7 with the ADTRAN terminal adapter was an oscillation of the RS/CS handshake sequence between the TA and the KIV-7. This was attributed to a 1-millisecond (ms) delay in the TA's response to RS, and was corrected by selecting CS "Forced On" in the TA configuration. An alternative solution which also worked in full duplex mode was to use a modified cable to the TA which connected the RS signal directly to the CS signal at the KIV-7, and did not connect either signal to the TA.

The second test configuration for the KIV-7 was to connect one Fireberd analyzer and KIV-7 unit to the RS-449 HSD port of an Inmarsat-B terminal, as shown in Figure 3. The second analyzer and KIV-7 were left connected to the ISDN TA, as before. These tests were conducted by placing an HSD data call from the Inmarsat-B terminal to one 64 kb/s port of the ISDN terminal adapter, attempting to complete crypto synchronization, and then performing tests with the data error analyzer. In this configuration, the KIV-7 would not achieve reliable automatic crypto sync in either the RED or NR sync mode. After much experimentation with RS-449 handshake lines, clocking options and other configuration parameters, it was determined that crypto synchronization of the KIV-7 in RED or NR modes could only be achieved reliably by manual intervention. A procedure was established in which the Inmarsat-B HSD call was placed with the KIV-7 devices at each end in the OFF-LINE mode. With the HSD call established, and a few seconds allowed for circuit stabilization, the KIV-7 units would be manually selected to ON-LINE mode. This method provided the most reliable method of achieving crypto sync, but has the obvious drawback of requiring manual intervention for placing a secure call.

During a discussion with technical personnel at Allied Signal Inc., it was learned that the OP2 sync mode was designed to be used with satellite circuit applications, and was more tolerant of the clock and data instabilities which can be encountered. Accordingly, further testing was performed with the KIV-7 devices operating in OP2 sync mode. In this mode, automatic crypto synchronization was reliably achieved after placing each Inmarsat-B HSD call, but it was noted that both KIV-7's would cycle through several synchronization attempts before stabilizing when each test call was placed. The Fireberd analyzers again indicated valid, error-free data circuits after crypto sync had stabilized. It was indicated by the Allied

Signal representative that the OP2 mode might have a tendency to magnify the effect of any data errors contributed by the HSD data circuit, but this effect was not observed during the tests.

2.4 VideoLynxx Desktop Video Conferencing Terminal

The manual for the VideoLynxx unit [4] was not available until after these trials, hence most of the information discussed in this report was obtained by phone or fax from the manufacturer. The unit is a PC-based device, with external monitor, video camera, microphone, speaker, keyboard and mouse. It uses a Windows-based software video conferencing application, and has a special purpose dual high-speed data port provided by a custom card and cable. The interface cable terminates with two DB25M connectors which implement two RS-366 dialling ports, and two DB37M connectors which implement primary and secondary RS-449 DTE data ports. The initial configuration for testing the VideoLynxx terminals was to connect them in a point to point ISDN configuration using the Adtran Terminal Adapters in a similar configuration to that of Figure 2, with the FireBerds replaced by the VideoLynxx terminals.

Normal configuration of the unit is automatic answer mode, with transmit timing (TT) supplied by the DCE device. After start-up, the application idles in a not connected state, holding the DTE TR signal in a true state. When a valid RS-449 circuit is established, the application expects to see a single transition of the DCE RR signal to a true state. It responds by attempting to communicate with the remote unit, running through a set-up protocol which takes several seconds to complete at 64 kb/s, and results in a complete, full duplex audio and video link, displaying the status "Answered" on the video monitor.

The second test configuration for the VideoLynxx terminal was to connect one unit to the RS-449 HSD port of an Inmarsat-B terminal, as shown in Figure 4. The second VideoLynxx unit was left connected to the ISDN TA, as before. These tests were conducted by placing an HSD data call from the Inmarsat-B terminal to one 64 kb/s port of the ISDN terminal adapter. These tests with the VideoLynxx over an actual satellite circuit indicated that it is quite sensitive to the stability of the RS-449 synchronous data circuit. If the RR signal from the DCE device is allowed to cycle, or the data link is momentarily corrupted during the call setup phase, the video application software at one or both end of the link will tend to malfunction, and require the application to be re-started before another video call is attempted. The effect of this sensitivity is quite severe, since the HSD circuit established by the Inmarsat B terminal can be quite unstable for the first few seconds of a call, indicated by occasional cycling of the RR signal supplied to the RS-449 DTE device.

The third test configuration for the VideoLynxx terminals incorporated the KIV-7 crypto units discussed in section 2.3 above to implement a secure video conferencing circuit, and is shown in Figure 5. This is similar to the KIV-7 test configuration shown in Figure 3, with the FireBerd analyzers again replaced by the VideoLynxx terminals. These secure mode video conferencing tests were subject to the same RS-449 circuit stability problems discussed in the previous paragraph, with the effect being somewhat magnified by the OP2 synchronization cycling of the KIV-7 cryptos. Test results are further discussed in section 3 of this report.

2.5 IMX-6L Inverse Multiplexer

Several configurations were considered for providing a secure video conferencing circuit at 128 kb/s using two Inmarsat-B HSD links at 64 kb/s each. A configuration was selected which requires only one KIV-7 encryption device at each end of the link, but also requires a unit which can combine two or more low-speed data circuits into one composite high-speed port. This concept is the opposite of a conventional multiplexer, and is termed "Inverse Multiplexing". Figure 6 shows the configuration which was used to test this concept. Two RAD IMX-6L Inverse Multiplexers (IMUXes) were required as shown in [7]. One unit was used with two 64 kb/s channel connections made to the RS-449 HSD data ports of two Inmarsat-B terminals. The 128kb/s port side was connected to the black side of the KIV-7. The red side of the KIV-7 was connected to a Fireberd 6000 analyser.

On the fixed end of the circuit, two 64 kb/s channel connections were made from a second IMX-6L to the two ports of an ADTRAN ISDN terminal adapter. The 128 kb/s port side of the IMUX was again connected through the KIV-7 to another Fireberd analyzer. Both inverse multiplexers were configured to implement a standard BONDING1 protocol to combine the two Inmarsat data links into a 128 kb/s composite link. The unit connected to the Inmarsat-B terminals was selected to be the master unit, which would automatically control the type of call setup performed between itself and the slave unit at the ISDN end. The configuration of the IMUX units is summarized in Table 4.

Test were performed by placing two HSD data calls from the Inmarsat B terminals to the two ports of the ISDN TA. With both circuits in place, the master IMUX performed an initialization sequence using data channel 1, then added traffic on data channel 2. After several seconds of this initialization, both IMUXes enabled their data ports by raising the Receiver Ready (RR) signals, and began to pass 128 kb/s synchronous data. The KIV-7 units responded by automatically achieving crypto sync, and provided secure 128 kb/s data to the data analyzers being used as DTE equipment. The data analyzers on the ports were used to confirm error-free data communications after the KIV-7's achieved sync.

Further testing with different sync modes on the KIV-7 units confirmed that operation of the 128 kb/s IMUX circuit was stable enough to support reliable KIV-7 synchronization in RED, NR and OP2 modes. The buffering provided by the IMUX units between the Inmarsat/ISDN data links and the KIV-7's, combined with the several second delay imposed by the IMUX initialization sequence before enabling the 128 kb/s link had the effect of enhancing the circuit reliability.

2.6 CS8000 Voice/Data Multiplexer

In addition to secure video conferencing tests, work was also undertaken to evaluate the performance of the CS8000 Time Division Multiplexer when used with cryptographic equipment. The VideoLynxx units shown in Figure 5 were replaced by CS8000 multiplexers. Cabling to the multiplexer network ports required non-standard adapter cables to convert RS-422 signal lines from the CS8000 DB25 network port connectors to standard RS-449 DB37M connectors. These in turn connected to a second set of adapter cables converting standard RS-449 DB37 pinout to the non-standard pinout used on the KIV-7 red side DB37F connectors.

The Fireberd 6000 analyzers were attached to one of the Intelligent Bandwidth Allocation (IBA) data ports on each mux as shown in Figure 7. A pair of HP1645A data error analyzers was also attached to a second sub-rate data port on each mux. Two voice

cards on the mux connected to the Inmarsat-B terminal were configured as FXS to accept local handsets, and a STU-III phone and a normal touch tone phone were attached. The corresponding two voice cards on the mux connected to the ISDN TA were configured as FXO to accept regular Public Switched Telephone Network (PSTN) lines, and connected to local RJ-11 telephone jacks. A second STU-III phone was connected to another PSTN line co-located with the Inmarsat-B terminal for test purposes. Multiplexer configuration parameters for these tests are summarized in Table 5.

The KIV-7 cryptos were configured for the robust OP2 synchronization mode, and were left in the ON-LINE or automatic re-sync state for the mux testing. Tests were performed by placing a single HSD 64 kb/s data call from the Inmarsat-B terminal to the ISDN TA, waiting for automatic crypto sync after the data circuit was established, then observing the performance of the CS8000 multiplexers. Results of several repeated tests showed that unassisted crypto sync was reliably achieved after two or more re-sync cycles, followed shortly by multiplexer sync indication. The data and voice ports attached to the multiplexers were successfully tested for error-free operation after some initial problems with mux configuration commands. The Fireberd analyzers on the IBA data port were also able to show the variation in allocated bandwidth by displaying Receive Timing (RT) changes as one or more voice lines were activated by placing test phone calls. More information on this and other performance features of the CS8000 multiplexer is available in [8].

3. SECURE COMMUNICATIONS TESTS

With the individual pieces of equipment characterized, it was possible to plan a series of secure communications tests which would have the best chance of reliable operation. A total of six configurations were prepared, of which the first four were fully tested, and the last two were partially tested and documented in this report. The configurations are summarized in the following list, and are discussed in more detail below:

1. 64 kb/s Manual Call Video Conf., Auto OP2 Encryption
2. 64 kb/s AutoAnswer Video Conf., Manual RED Encryption
3. 2x64 kb/s AutoAnswer Video Conf., Manual RED Encryption
4. 128 kb/s AutoAnswer Video Conf., Auto RED Encryption
5. 64 kb/s Double Hop Manual Call Video Conf., Auto OP2 Encryption
6. 64 kb/s DVCN Access, AutoAnswer, Auto OP2 Encryption

Individual configuration setup parameters for each piece of equipment used in these tests are documented in Tables 1-5 of this report, with particular changes made only as discussed in the sections below for the purposes of each test.

3.1 64 kb/s Manual Call Video Conferencing, Auto OP2 Encryption

This configuration is the most basic one, and allows for video conferencing with a minimum of equipment at a rate supported by a single HSD circuit on an Inmarsat-B terminal. The complete end-to-end circuit is shown in Figure 5. All calls are originated from a field location by a VideoLynxx unit, connected through a KIV-7 crypto to an Inmarsat-B satellite terminal. The SATCOM call is then routed from the Inmarsat earth station vis ISDN circuits to a Terminal Adapter at the destination site, where the call terminates via another KIV-7 Encryption unit on a second VideoLynxx terminal. The particular configuration parameters required for this test are as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	1	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x64, CH1, Autoanswer OFF
KIV-7	2	3	Sync: OP2, Mode: ON-LINE
IMX-6L	0	4	Not used
CS8000 Mux	0	5	Not used
Adtran TA	1	2	No changes

This configuration was designed to provide for unattended operation of the KIV-7 comsec units, while requiring manual intervention at each end of the circuit to control the VideoLynxx operation. Calls were placed from the Inmarsat B handset, followed by a few seconds wait for circuit stabilization. Any call answer windows appearing on the VideoLynxx monitor were cleared with the "Do Not Answer" button. When a stable circuit was indicated by the Inmarsat-B master handset and the KIV-7 ON-LINE TR indication, both VideoLynxx units were commanded to place a 1x64 kb/s data call. These calls were successfully completed in about 8 out of 10 attempts during these tests. Incomplete calls appeared to be the result of the two VideoLynxx units failing to complete the necessary initialization protocol over the secure data channel.

3.2 64 kb/s AutoAnswer Video Conferencing, Manual RED Encryption

This configuration also utilizes the minimum of equipment for a secure video conferencing call, and again requires only the single HSD data circuit from an Inmarsat-B terminal. The complete end-to-end circuit is identical to that described in section 3.1. The configuration parameters of the equipment required for this test have some changes from those in section 3.1, and are summarized as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	1	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x64, CH1, Autoanswer ON
KIV-7	2	3	Sync: RED, Mode: OFF-LINE
IMX-6L	0	4	Not used
CS8000 Mux	0	5	Not used
Adtran TA	1	2	No changes

This configuration provides for manual control of the crypto synchronization process, while leaving the VideoLynxx terminals in auto-answer mode. Calls were again placed from the Inmarsat B terminal master handset, followed by a few seconds wait for circuit stabilization. When a stable circuit was indicated by the handset display, the KIV-7 units were manually selected to ON-LINE mode at each end of the circuit. As soon as crypto sync was achieved, the Receiver Ready (RR) signal from each KIV-7 caused the corresponding VideoLynxx terminal to begin an automatic answer sequence to complete the video conferencing circuit. These calls were again completed in about 8 out of 10 attempts. Incomplete calls were generally attributed to the failure to achieve crypto sync during the call setup procedure. Recovery from failed call attempts occasionally required a re-initialization of the KIV-7 units by turning the Crypto Ignition Keys (CIK's) off and on.

3.3 2x64 kb/s AutoAnswer Video Conferencing, Manual RED Encryption

This is the first of two configurations designed to test the operation of the VideoLynxx equipment at a data rate of 128 kb/s. Additional equipment for these tests includes a second Inmarsat B HSD terminal, and a second pair of KIV-7 cryptographic units. The second HSD link is terminated on channel 2 of the same ISDN TA used in the previous tests. The entire configuration is shown in Figure 8, and takes advantage of the VideoLynxx feature which uses a "BONDING1" protocol to combine two separate 64 kb/s HSD links into a single 128 kb/s video conference link. A total of four KIV-7 units are used to provide separate data encryption on each HSD link. The configuration parameters for each piece of equipment used in this series of tests are as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	2	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x64, CH1 and CH2, Autoanswer ON
KIV-7	2	3	Sync: RED, Mode: ON-LINE
IMX-6L	0	4	Not used
CS8000 Mux	0	5	Not used
Adtran TA	1	2	CH 1 and 2 used

This configuration again provides for manual control of the crypto synchronization process, while leaving the VideoLynxx terminals in auto- answer mode. It was found that the VideoLynxx terminals would only perform a proper bonding of the two 64 kb/s circuits if selected for autoanswer mode. Calls were again placed from first one Inmarsat B terminal master handset, then the second followed by a few seconds wait for both circuits to stabilize. When both circuits were stable as indicated by the handset displays, the KIV-7 units on channel one were manually selected to ON-LINE mode at each end of the circuit, followed by the KIV-7 units on channel 2. As soon as crypto sync on channel one was achieved, the Receiver Ready (RR) signal from each KIV-7 caused the corresponding VideoLynxx terminal to begin an automatic answer sequence at 64 kb/s to complete the video conferencing circuit. When crypto sync on channel two was also complete, the VideoLynxx terminals automatically performed a bonding sequence to increase the data rate to a total of 128 kb/s.

As these calls were subject to the reduced reliability of two simultaneous HSD links, the success rate was somewhat lower. Calls at the full 128 kb/s rate were completed in about 5 out of 10 attempts. Incomplete calls were generally attributed to the failure to achieve crypto sync on one of the two channels during the call setup procedure, or to inconsistency in the stability of multiple HSD links. There were a number of occurrences in which at least one HSD call was intermittent, and had to be terminated and re-tried several times. This may have been the result of marginal performance in one Inmarsat-B terminal, interference effects in the experimental antenna sharing circuits, or allocation of a problem channel on the Inmarsat satellite. Recovery from failed call attempts occasionally required a re-initialization of the KIV-7 units by turning the Crypto Ignition Keys (CIK's) off and on.

3.4 128 kb/s AutoAnswer Video Conferencing, Auto RED Encryption

A second series of tests on secure HSD video conferencing was also performed at 128 kb/s, but some significant differences in circuit configuration were implemented. The configuration is similar to Figure 6, with the VideoLynxx terminals replacing the FireBerd Analyzers. Two inverse multiplexers (IMUX'es) were added to the configuration to perform the bonding from two 64 kb/s links into one 128 kb/s data circuit. On the remote side, one IMUX was installed with two 64 kb/s data channels connected to the two Inmarsat-B terminal HSD connectors. The high-speed, or port side of the IMUX was connected through a KIV-7 to channel one of the VideoLynxx terminal.

On the ISDN side of the link, the second IMUX was installed with two 64 kb/s data channels connected to the two channels of the ADTRAN TA. Again, the high-speed side of the IMUX was connected through a second KIV-7 to channel one of the fixed site VideoLynxx terminal. This approach permitted the use of only two KIV-7 encryption units, operating in the 128 kb/s portions of the link. The VideoLynxx units were configured to operate on channel one only, with their data rates set to 128 kb/s. The configuration parameters for this test series are listed as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	2	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x128, CH1, Autoanswer ON
KIV-7	2	3	Sync: RED, Mode: ON-LINE
IMX-6L	2	4	No changes
CS8000 Mux	0	5	Not used
Adtran TA	1	2	CH 1 and 2 used

This configuration was designed to take advantage of the stabilizing influence of the IMX-6L inverse multiplexers (IMUXs) to provide for a fully automatic video conference call setup. The KIV-7 units were left in ON-LINE mode, meaning that they would automatically attempt crypto sync when the IMUX provided an RR signal. The VideoLynxx units were left in auto answer mode so that they would automatically perform call initialization and setup when the KIV-7 provided an RR signal.

Testing was performed by placing first one, and then a second HSD call from the Inmarsat B terminal master handsets. When the circuits were established, the master IMUX at the remote end executed a BONDING protocol with the slave IMUX at the ISDN end of the link. After several seconds of BONDING setup, both IMUXs provided RR signals to their respective KIV-7 cryptos, which initiated the crypto synchronization process at 128 kb/s. After another few seconds for this process, the KIV-7s passed the RR signals to the VideoLynxx units, which in turn executed their automatic answer sequences to establish the video conference call at 128 kb/s.

As these calls were subject to the reduced reliability of two simultaneous HSD links, the success rate was somewhat lower than for a single 64 kb/s video conference call, but was higher than the previous tests using four KIV-7 units to separately encrypt the two HSD links. The effect of the IMUX units was to provide a more reliable BONDING protocol on the two HSD links, and present the KIV-7s with a single, more stable 128 kb/s link for encryption. The VideoLynxx units also performed more reliably without having to perform the BONDING protocol as part of the video conference call setup.

Calls through the IMUXs at the 128 kb/s rate were completed in about 7 out of 10 attempts. Incomplete calls were generally attributed to inconsistency in the stability of multiple HSD links as discussed in the previous section. The IMUX units performed well in the presence of these inconsistent data links by sensing the failures automatically, and re-trying the BONDING procedure when the HSD links were restored. The interface to the KIV-7 on the high speed side of each IMUX was handled with sufficient delay in the cycling of the RR signal to allow the cryptos to cleanly drop and re-establish sync in response to circuit outages. This feature meant that recovery from failed call attempts only rarely required a manual re-initialization of the KIV-7 units by turning the Crypto Ignition Keys (CIK's) off and on.

3.5 64 kb/s Double Hop Manual Call Video Conferencing, Auto OP2 Encryption

This configuration was the only test done to evaluate the performance of the VideoLynxx terminals over a double hop satellite circuit. The complete end-to-end circuit is shown in Figure 9, where it can be seen that the ISDN termination at one end of the link shown in Figure 5 has been replaced by a second Inmarsat terminal. Calls were originated from either Inmarsat terminal using a special dialling sequence which routed the call through the Inmarsat Land Earth Station (LES) and directly back over a second satellite link to the second Inmarsat terminal. The configuration parameters required for this test are as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	2	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x64, CH1, Autoanswer OFF
KIV-7	2	3	Sync: OP2, Mode: ON-LINE
IMX-6L	0	4	Not used
CS8000 Mux	0	5	Not used
Adtran TA	0	2	Not used

This configuration was also designed to take advantage of the OP2 unattended operation mode of the KIV-7 comsec units, while requiring manual intervention at each end of the circuit to control the VideoLynxx operation. Calls were placed from one Inmarsat B terminal master handset, followed by several second wait for double hop circuit stabilization. When stable circuits were indicated by both terminal master handsets, and both KIV-7 units displayed ON-LINE TR crypto sync status, the two VideoLynxx units were commanded to place a 1x64 kb/s call. These calls were completed in less than 5 out of 10 attempts. Incomplete calls were attributed to the effects of the longer double hop delay on the initialization protocol exchange between the VideoLynxx terminals.

3.6 64 kb/s DVCN Access, AutoAnswer, Auto OP2 Encryption

This configuration for secure video conferencing was implemented several months after the test described above. The purpose of this test was to evaluate the feasibility of connecting a low-rate 64 kb/s secure video conferencing link from a remote site via Inmarsat-B HSD/ISDN into the Defence Video Conference Network (DVCN) site at Tunneys Pasture. This link presented unique problems because of the mismatch between the data rates of the 64 kb/s remote unit and the 384 kb/s standard DVCN interface. The solution implemented for this demonstration was to terminate the 64 kb/s Inmarsat-B HSD/ISDN circuit from the remote VideoLynxx terminal at the Defence Integrated Services Digital Network (DISDN) node in the Tunneys Pasture Communications Center. From this location, the 64 kb/s circuit was routed to a V.35 interface on the DVCN secure Annex in the same building, and terminated at a second KIV-7 comsec unit and a VideoLynxx terminal. This configuration allowed for a baseband video and audio full duplex cross connection from the 64 kb/s VideoLynxx terminal to a standard 384 kb/s DVCN Codec, which in turn supplied the necessary secure interface into the DVCN. Appropriate security waivers were authorized to permit this demonstration to take place over the operational DVCN system.

Figure 10 shows the entire configuration used for this trial. The configuration parameters used were as follows:

Equipment	Qty	Setup Table	Remarks
Inmarsat B Terminal	1	1	No changes
VideoLynxx Terminal	2	-	Rate: 1x64, CH1, Autoanswer ON
KIV-7	2	3	Sync: OP2, Mode: ON-LINE
IMX-6L	0	4	Not used
CS8000 Mux	0	5	Not used
Adtran TA	1	2	DTE1 Connector: V.35

This configuration was designed for unattended operation of both the KIV-7 comsec units, but required manual control of the VideoLynxx terminals. Calls were placed from the Inmarsat B handset, followed by a few seconds wait for circuit stabilization. When a stable circuit was indicated by the Inmarsat B master handset and the KIV-7 ON-LINE TR

indicators, both VideoLynxx units were commanded to establish a 1x64 kb/s data call. With the 64 kb/s video conference circuit established, the DVCN codec was connected into a 384 kb/s standard video conference with a second DVCN site located in a conference room on the third floor of the building. This secure 64 kb/s video conference link to the DVCN was successfully established several times to assess the reliability of the circuit, and to demonstrate its performance to senior DND staff members.

There were two observations made from this trial. First, there was an unavoidable requirement for manual intervention in setting up the 64 kb/s VideoLynxx circuit on each call. This was a result of using the DISDN system to route the ISDN call to the DVCN Annex. The DISDN could not replicate cycling of the Receiver Ready signal from the ISDN Terminal Adapter to the KIV-7 located in the DVCN Annex, and hence the VideoLynxx terminal had no handshake signal to indicate an incoming call. Second, there was an unusually long delay observed between transmission and response during the DVCN video conference. This delay was in excess of 2 seconds, and was significantly longer than expected for a single hop satellite circuit. The excess delay was attributed to processing delays encountered in the baseband cross-connection between the 64 kb/s VideoLynxx and the 384 kb/s DVCN Codec.

4. HSD TESTS USING BOTH KG-84C AND KIV-7 ENCRYPTION DEVICES

A later series of tests was performed to evaluate the performance of the KG-84C Encryption unit over the Inmarsat-B HSD circuits. This test plan was carried out in early 1999 at the Satcom Terminal Facility in Bldg T85 at DREO. The intention was to determine if any special procedures were required to use the older KG-84C Crypto in place of the KIV-7 for some of the tests described in sections 2 and 3 of this report. No manual was available for configuring the KG-84C units, but assistance was provided by personnel from the DND Comsec group for these trials. The important consideration is that the KIV-7, described as an Embeddable KG-84 Comsec Module [5] is fully compatible with the KG-84C unit, and most operating modes and option selections described in [5] for the KIV-7 have an equivalent setting in the KG-84C. Table 6 summarizes the KG-84C settings used for these tests.

4.1 Single-Hop Crypto Compatibility Testing

The first test performed in this series was to verify that the KG-84C would reliably achieve crypto sync, and pass full duplex traffic when connected with a KIV-7. Figure 11 shows the configuration chosen for this test. The KG-84C was fitted with a Crypto Interface Device for RS-530 (CID-530) on both red and black interfaces. This provided for direct connection of the black side to the Inmarsat-B terminal through an RS-449 to RS-530 adapter cable, and the red side to the FireBerd 6000 through a standard RS-530 cable.

HSD links were successfully initiated from both the Inmarsat-B terminal and the ISDN TA. Experimentation with the standard RS-530/RS-449 handshake lines indicated that both RS and TR signals were required from the FireBerd DTE equipment, and were passed transparently through the KG-84C crypto to enable the HSD circuit at the Inmarsat B terminal. The KG-84C would automatically achieve crypto sync with the KIV-7 when the RR signal was asserted by the terminal after establishing an HSD satellite link. There was no significant bit error measurement (BER) observed on the FireBerd analyzers monitoring both ends of the full duplex HSD circuits. Calls were completed in better than 9 out of 10 attempts, indicating a consistent and reliable circuit.

The second test configuration involving KG-84C devices is shown in Figure 12. For this test, a second KG-84C was connected to the ADTRAN TA on the ISDN end of the link, replacing the KIV-7 crypto. Again the two KG-84C crypto devices reliably achieved crypto sync and passed error free data over HSD dial-up links established from either end of the test circuit. For this configuration as well, calls were completed in better than 9 out of 10 attempts.

4.2 Double-Hop Crypto Compatibility Testing

The final series of tests with the KG-84C cryptos was intended to evaluate their performance over a double-hop satellite HSD link. This type of link is achieved by dialing directly from one Inmarsat-B terminal to a second terminal. The user data originating from one terminal has to pass over one satellite circuit to reach the Inmarsat host earth station, where it is retransmitted over a second link to the second terminal. This type of data circuit is subject to twice the normal path delay, and to the accumulated BER effects of two satellite links. Figures 13 and 14 show the crypto configurations which were tested. In both cases, the two crypto devices achieved reliable crypto sync after double-hop HSD links were established, and passed error free, full duplex 64 kb/s data between the two FireBerd

analyzers. Double hop path delays were observed at nearly 1.0 seconds, with no negative effect on the crypto synchronization process. The quality of both Inmarsat-B HSD links was high enough that no measurable BER could be detected, and calls were completed in better than 8 out of 10 attempts.

4.3 Single and Double-Hop Local Area Network Extension Testing

With the BER and crypto sync testing completed, some additional tests were undertaken. The FireBerd analyzers shown in Figure 11 were removed from the test setup and replaced at both ends by Cisco Local Area Network (LAN) Routers. Figure 15 shows a typical configuration for these tests. A Laptop control computer was attached to one of the routers as a test device. The purpose of this test configuration was to determine the feasibility of using the 64 kb/s HSD satellite link as a LAN extension circuit, allowing two segments of a Transmission Control Protocol/Internet Protocol(TCP/IP) network to be interconnected for remote access to standard network services such as File Transfer Protocol (FTP), internet and e-mail.

The configuration was tested by using the laptop control computer to command one router to Ping the IP address of the second router at the far end of the link. This is a simple IP test which generates a sequence of inquiry packets directed at the target IP, and logs the time and error status of each response packet. Successful receipt of Ping responses by the originating router indicates a valid network connection to the target device. As expected with this configuration, the response times over the HSD link were in excess of 1000 ms, reflecting the effect of both transmit and receive satellite path delays, plus 100-200 ms of buffer delays through the routers. The crypto configuration similar to Figure 12 was also tested in this manner, with similar results. Finally, a brief test of a double-hop LAN extension was successfully performed using the routers in place of the FireBerds in Figure 13, and the expected increase in round-trip response times to about 1800 ms was observed on the router Ping tests.

Further testing of this LAN extension service over Inmarsat HSD links was discussed with DTSES staff, and may include actual FTP file transfers between LAN segments and remote access to the Defence Wide Area Network(DWAN) e-mail and intranet services.

5. CONCLUSIONS

This report has described the results of a series of 64 kb/s and 128 kb/s secure data communications tests with a variety of DND crypto and terminal equipments. A number of issues were raised with respect to equipment interface standards, and solutions to most of these have been proposed and tested. Configuration summaries for most of the equipment tested have been listed in Tables 1 through 6 at the end of this report.

The HSD to ISDN communications mode of the Inmarsat-B terminals offers DND a secure, reliable and convenient means to establish 64 kb/s data links from virtually any location on the earth having coverage by the Inmarsat satellite system. Data links supporting 64 kb/s and 128 kb/s secure video conferencing, secure multiplexed voice and data, and secure LAN extension services have been successfully demonstrated.

For low-rate video conferencing from field units, the results of these tests suggest that the relatively minor increase in video resolution achieved by using a 128 kb/s link does not justify the increased complexity and cost of the additional equipment required. In addition, all of the different 128 kb/s tests described in this report suffered from the reduced circuit reliability which results from using more than one Inmarsat HSD circuit simultaneously. The probability of a successful call is reduced to the product of the probabilities for each individual circuit used.

For best results in secure low-rate video conferencing, the recommended configuration is that discussed in section 3.1 of this report, a 64 kb/s manually controlled video conference call, with KIV-7 cryptos set for OP2 encryption mode. This configuration provides for positive control of the circuit by allowing the operator to establish a stable Inmarsat HSD link before activating the video conference equipment.

The main drawbacks to the use of the HSD service are the relatively high cost per minute of an HSD call, and the fact that the service is provided on a strictly first-come, first-served basis. This means that, in an emergency situation involving DND, there is no guarantee of obtaining HSD service since the probability of blocked calls is likely to increase sharply due to demand from media and other civilian agencies responding to the same emergency.

6. REFERENCES

[1] J. Brassard and C.Somers, "Inmarsat B High Speed Data Trial Report", Bell Canada Signature Service Report, March 1996.

[2] Roger L. Freeman, "Reference Manual for Telecommunications Engineering, Second Edition", John Wiley & Sons, 1994.

[3] "LYNXX Operator's Manual - LYNXX Transportable Inmarsat-B Earth Station", California Microwave Mobile Satellite Products document No. 202-TM-00002, revised June 1995.

[4] "VideoLynxx VTC-64P Portable Video Teleconferencing System User's Manual", California Microwave Mobile Satellite Products preliminary document, January 1997.

[5] "Embeddable KG-84 COMSEC Module (KIV-7) USER'S MANUAL", Allied Signal Inc. Communications Systems document No. 4065544-0201, revised March 1994.

[6] "ISU 2x64 Dual Port ISDN Service Unit User's Manual", ADTRAN, Inc. document No. 61200.051L1-1, March 1996.

[7] "IMX-6L Inverse Multiplexer Operator's Manual", RAD Data Communications Ltd. Pub. No. 441-20-12/94, 1994.

[8] "CS8000 Clarity Series Voice/Data Multiplexer", Pacific Communication Sciences Inc. document No. 299-010, revision F, March 1993.

[9] "FIREBERD 6000 Reference Manual", Telecommunications Techniques Corporation document No. 50-12120-01, revision L, January 1996.

[10] "FIREBERD 6000 User's Guide", Telecommunications Techniques Corporation document No. 50-12136-01, revision D, June 1995.

APPENDIX A

FIGURES

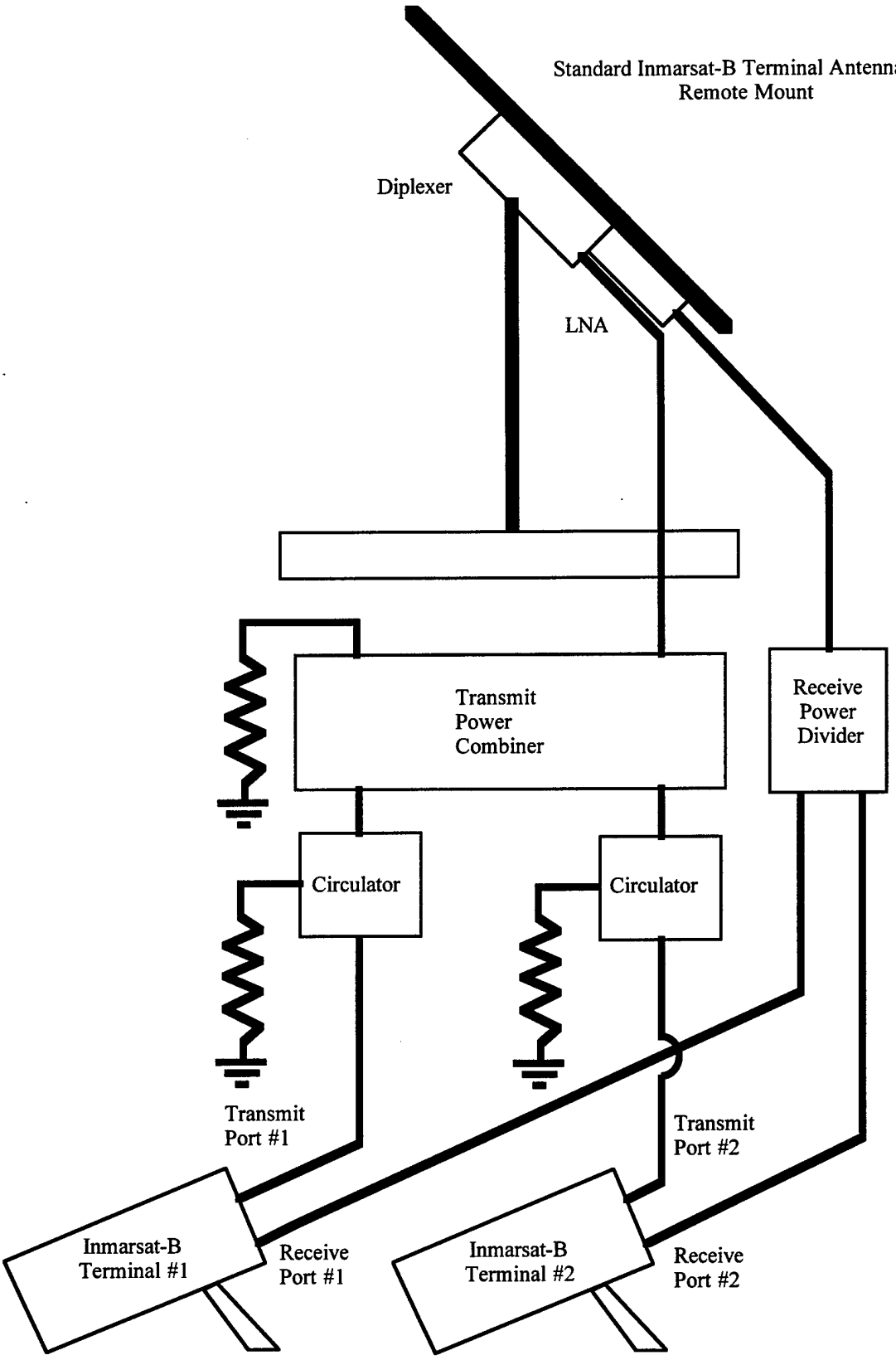

Figure 1
RF Combiner Circuit for Two Inmarsat B
Terminals Sharing One Common Antenna

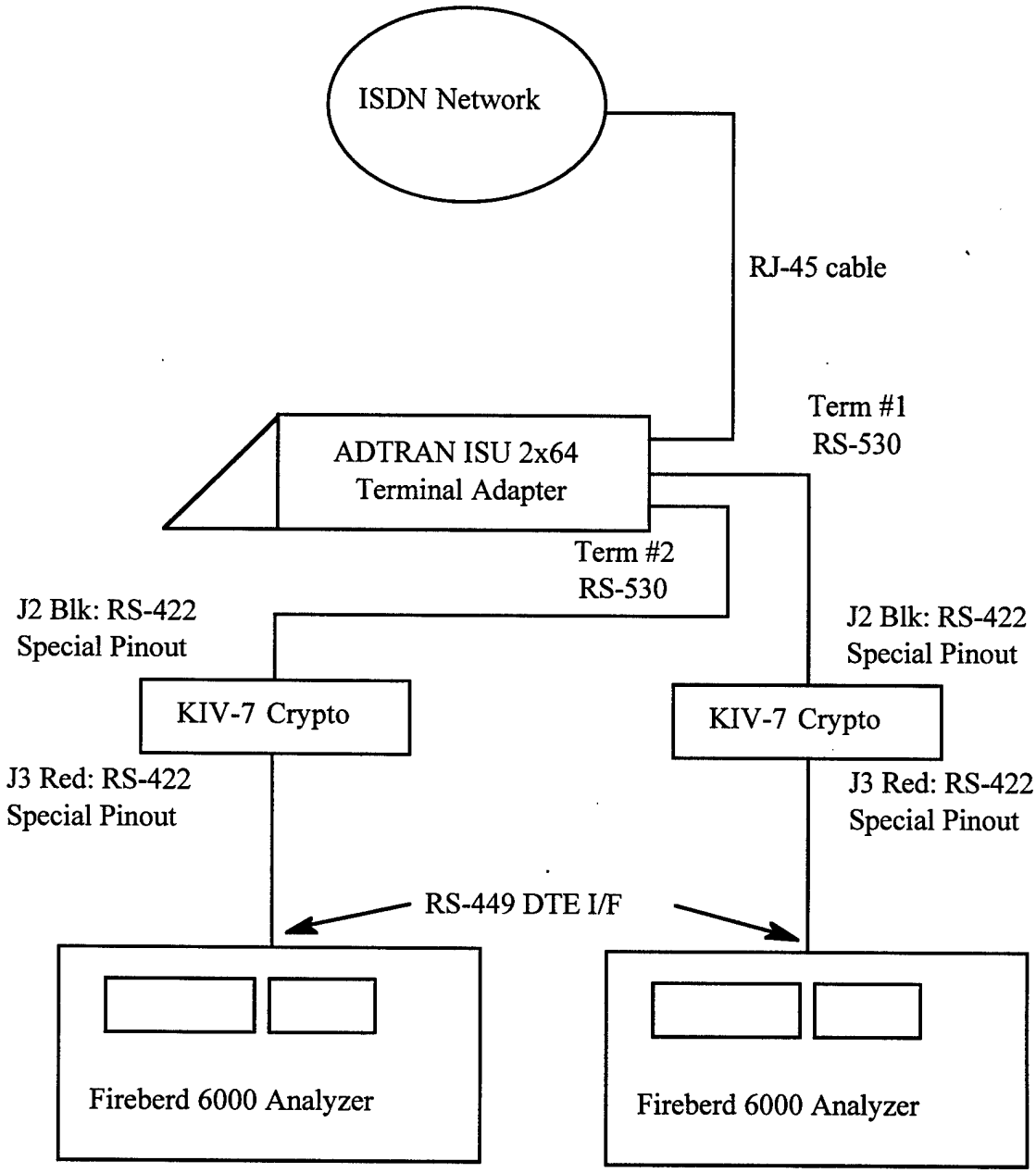

Figure 2
Basic KIV-7 Test with Two ISDN Connections

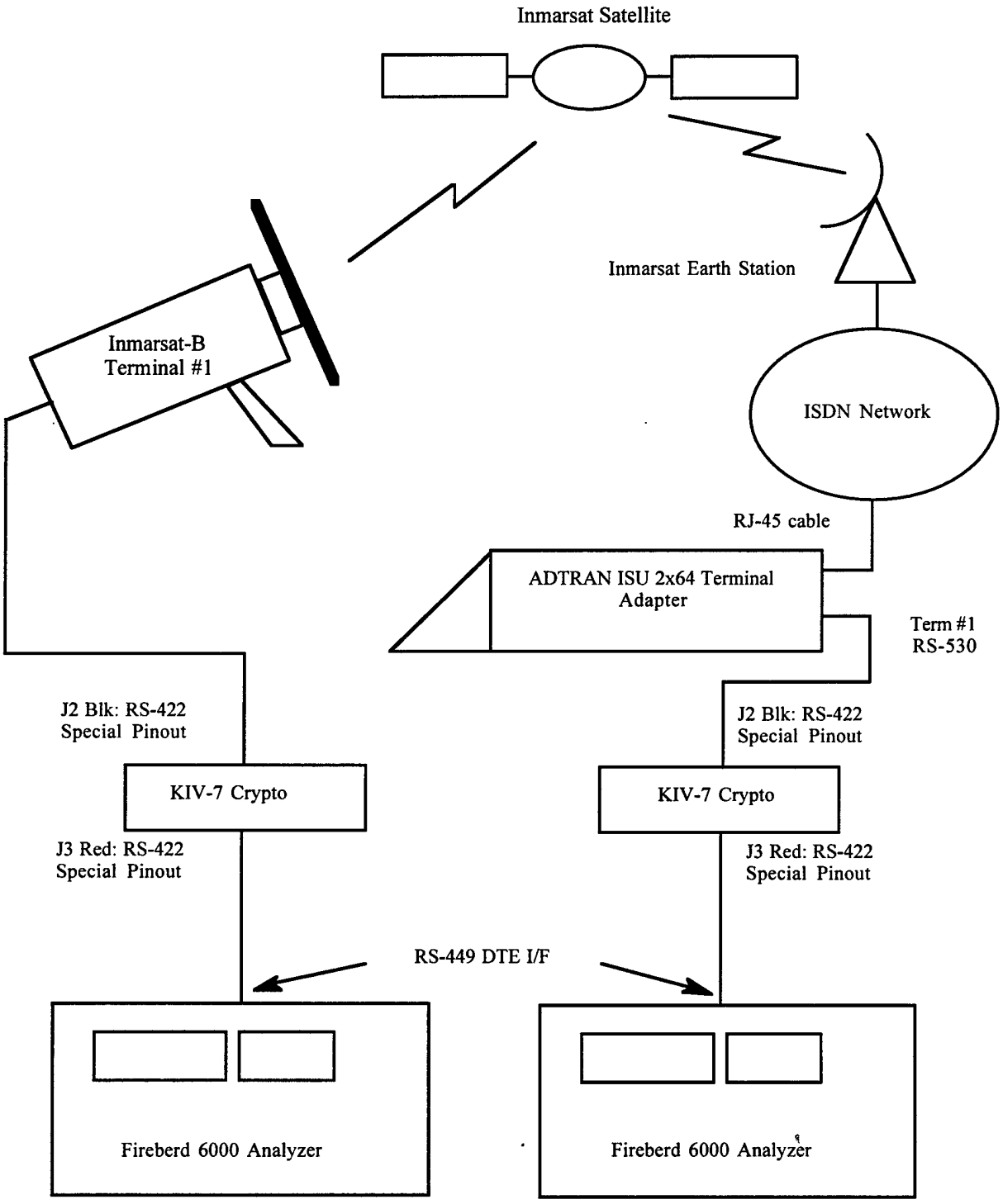

Figure 3
KIV-7 Test with Inmarsat HSD to ISDN Link

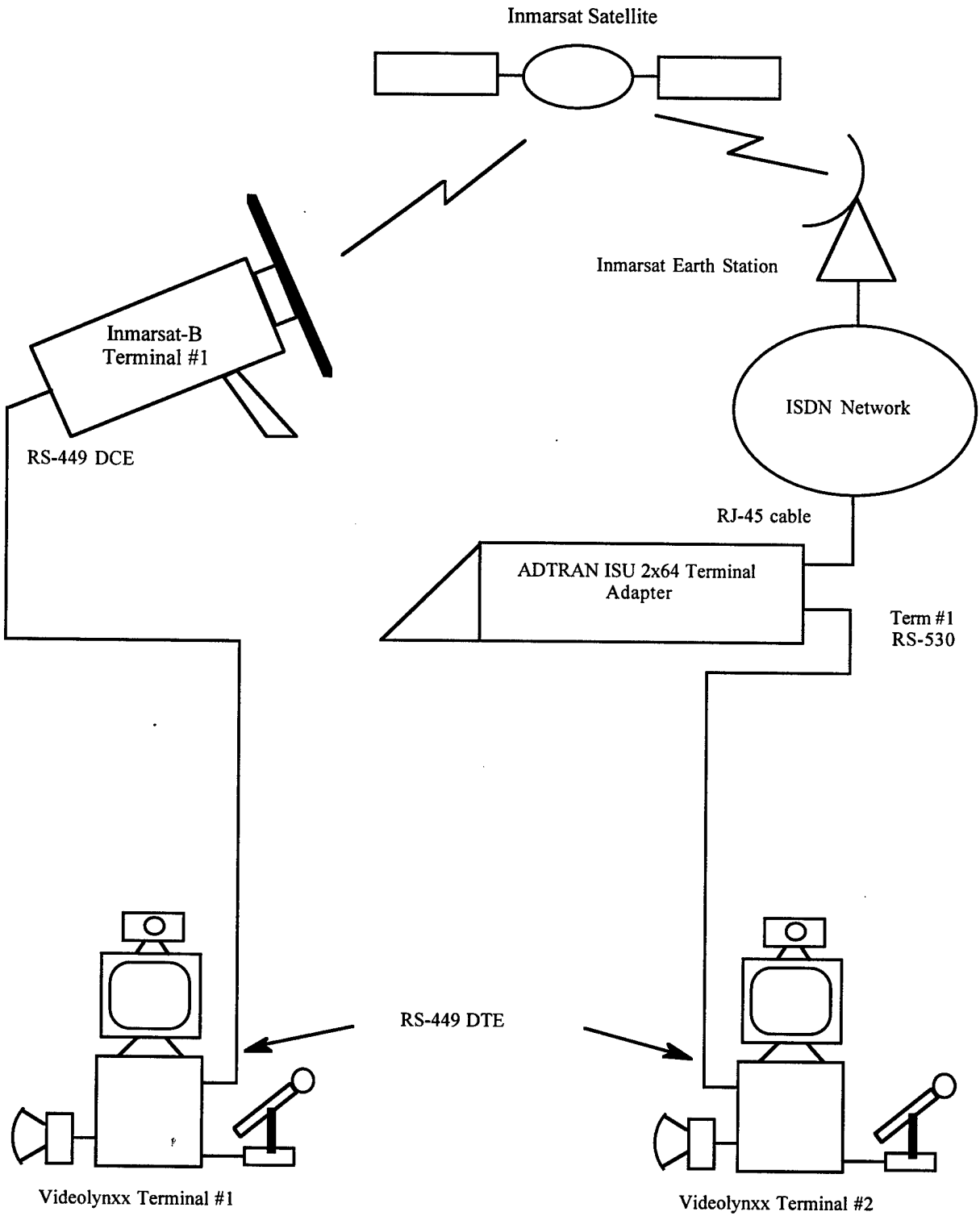

Figure 4
VideoLynxx Test with Clear 64 kb/s Inmarsat HSD to ISDN Link

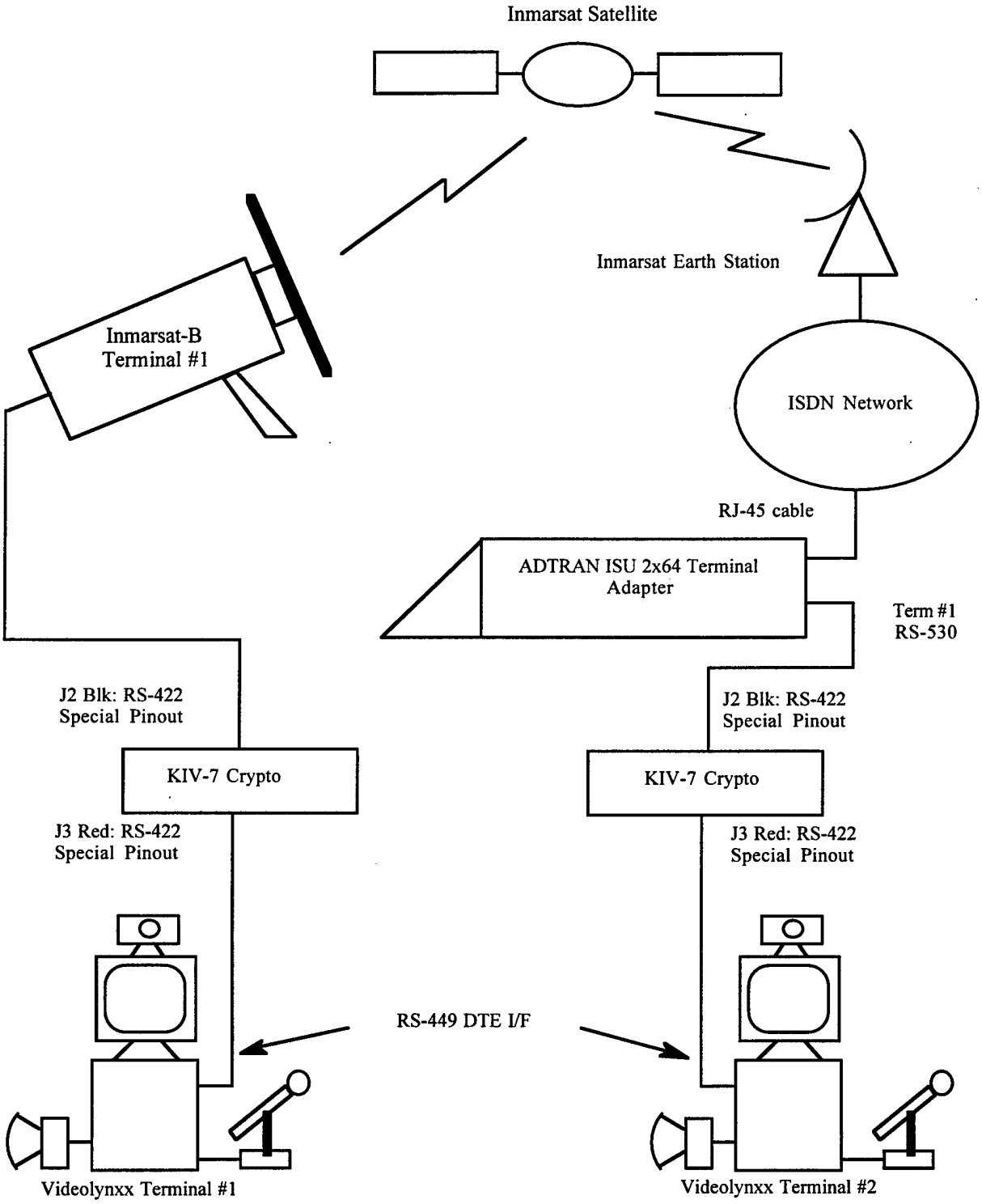

Figure 5
VideoLynxx Test with Secure 64 kb/s Inmarsat HSD to ISDN Link

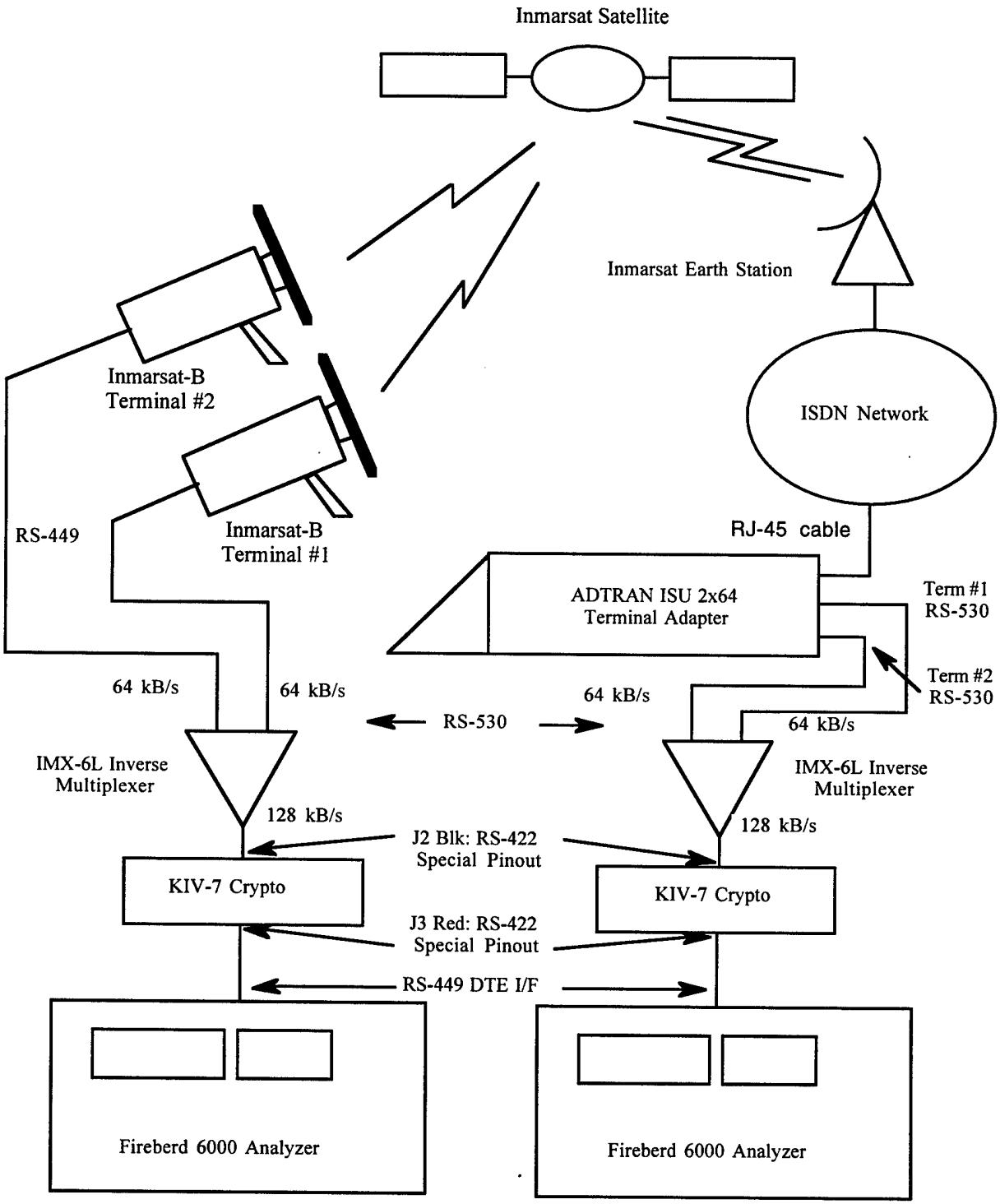

Figure 6
Inverse Multiplexer Test with Two 64 kb/s HSD to ISDN Links

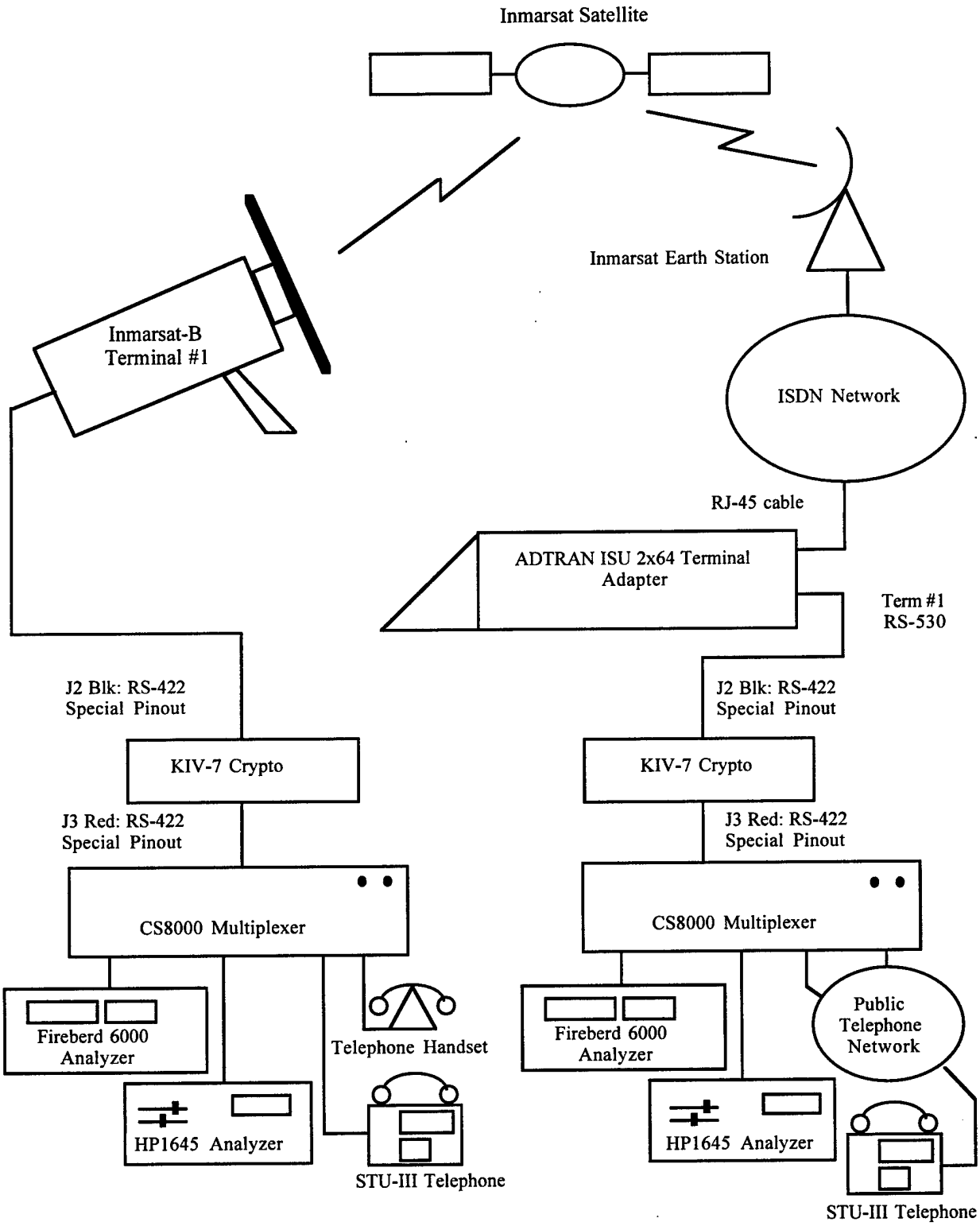

Figure 7
CS8000 Multiplexer Setup for Secure Voice and Data Test

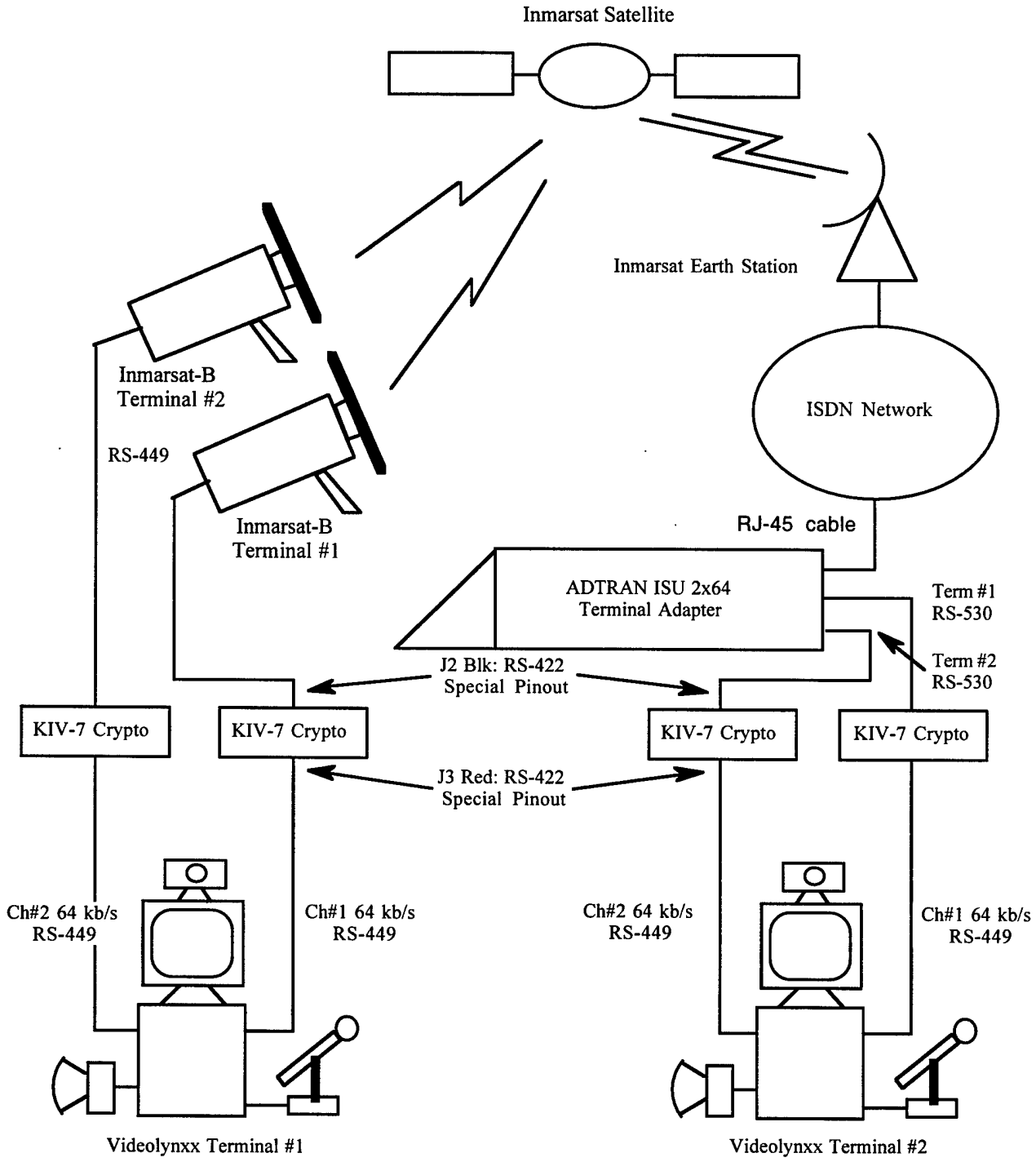

Figure 8
128 kb/s Video Conferencing Test Using Internal VideoLynxx
BONDING Protocol

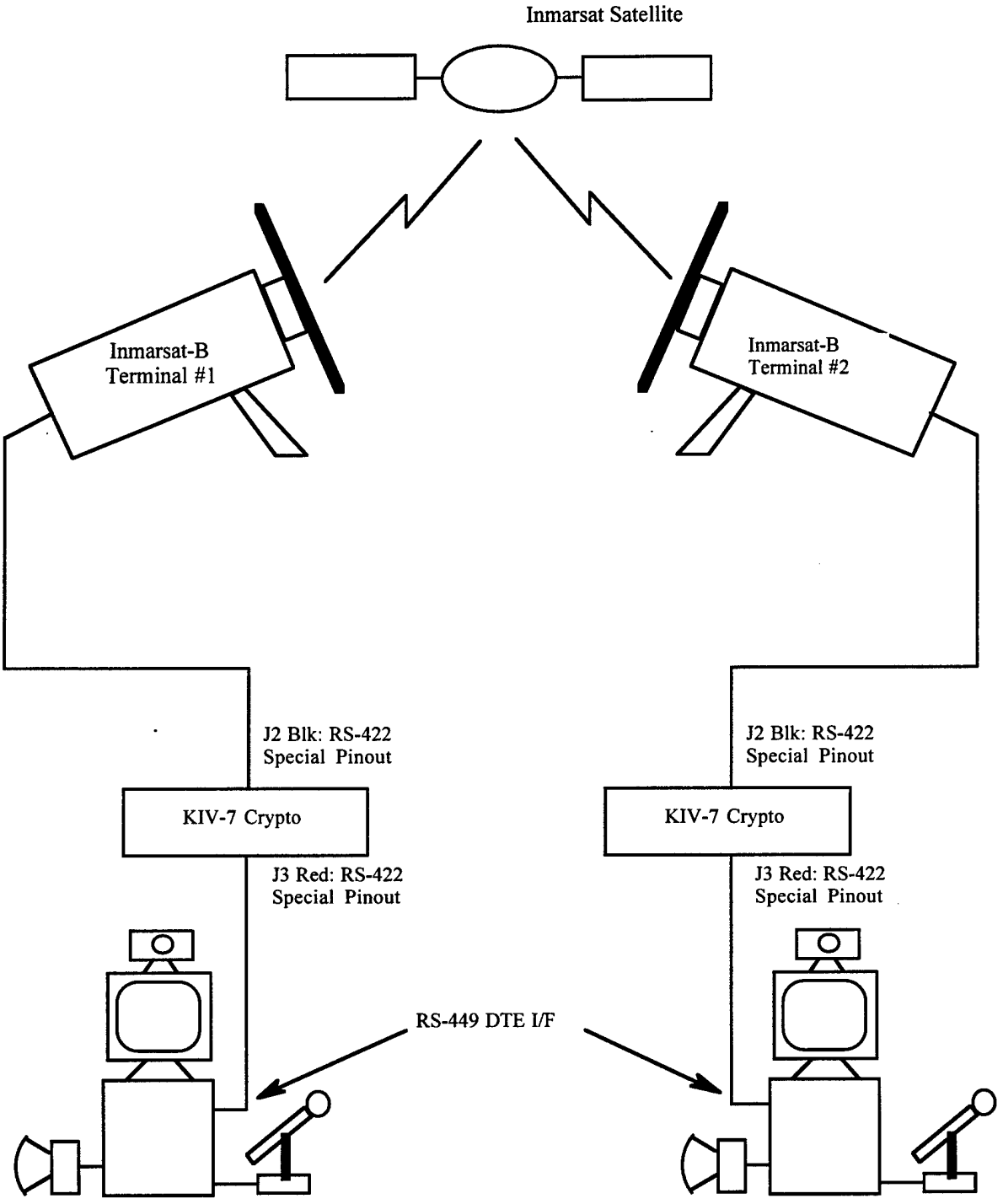

Figure 9
Double-Hop 64 kb/s VideoLynxx Test

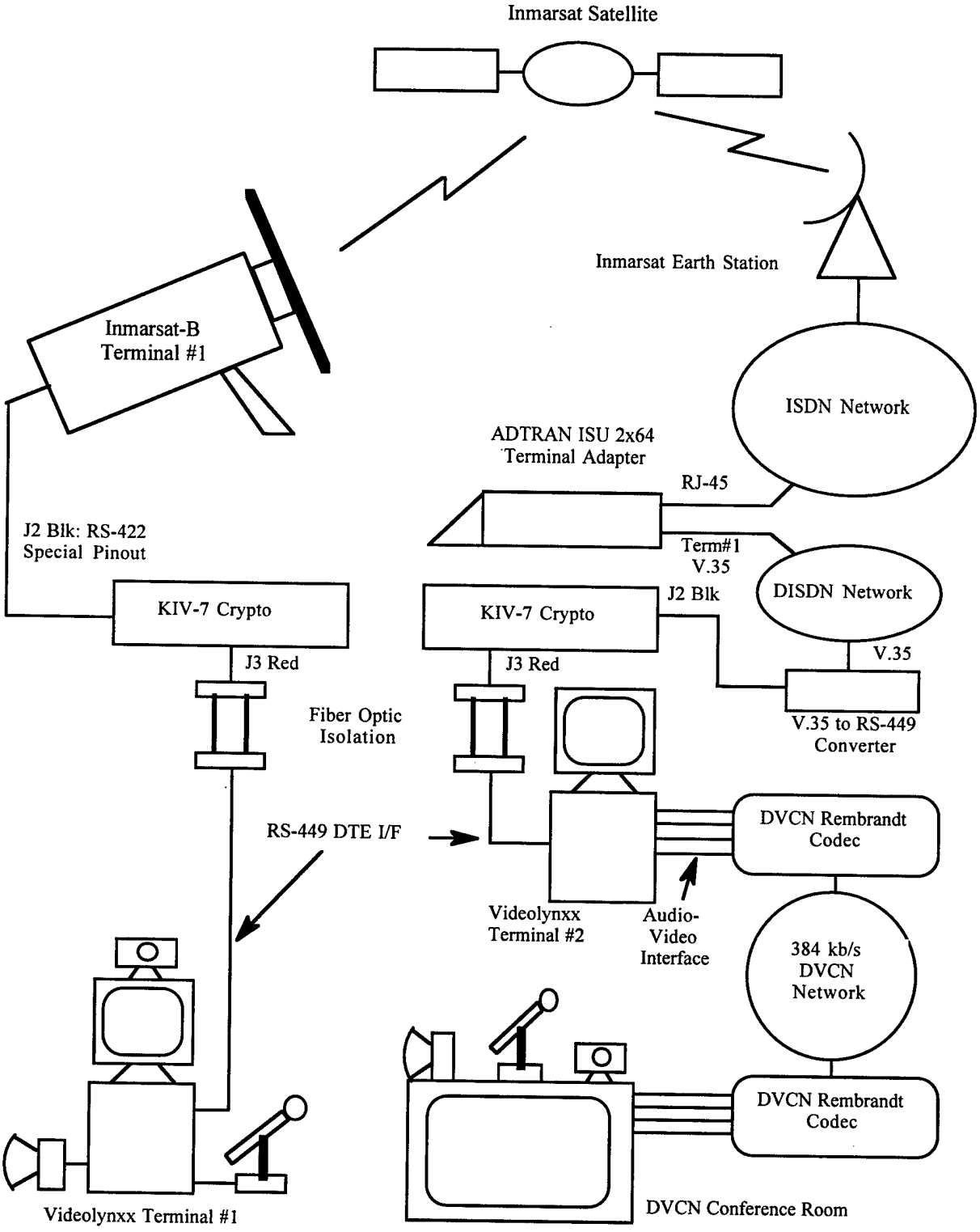

Figure 10
VideoLynxx to DVCN Secure Video Conferencing Test

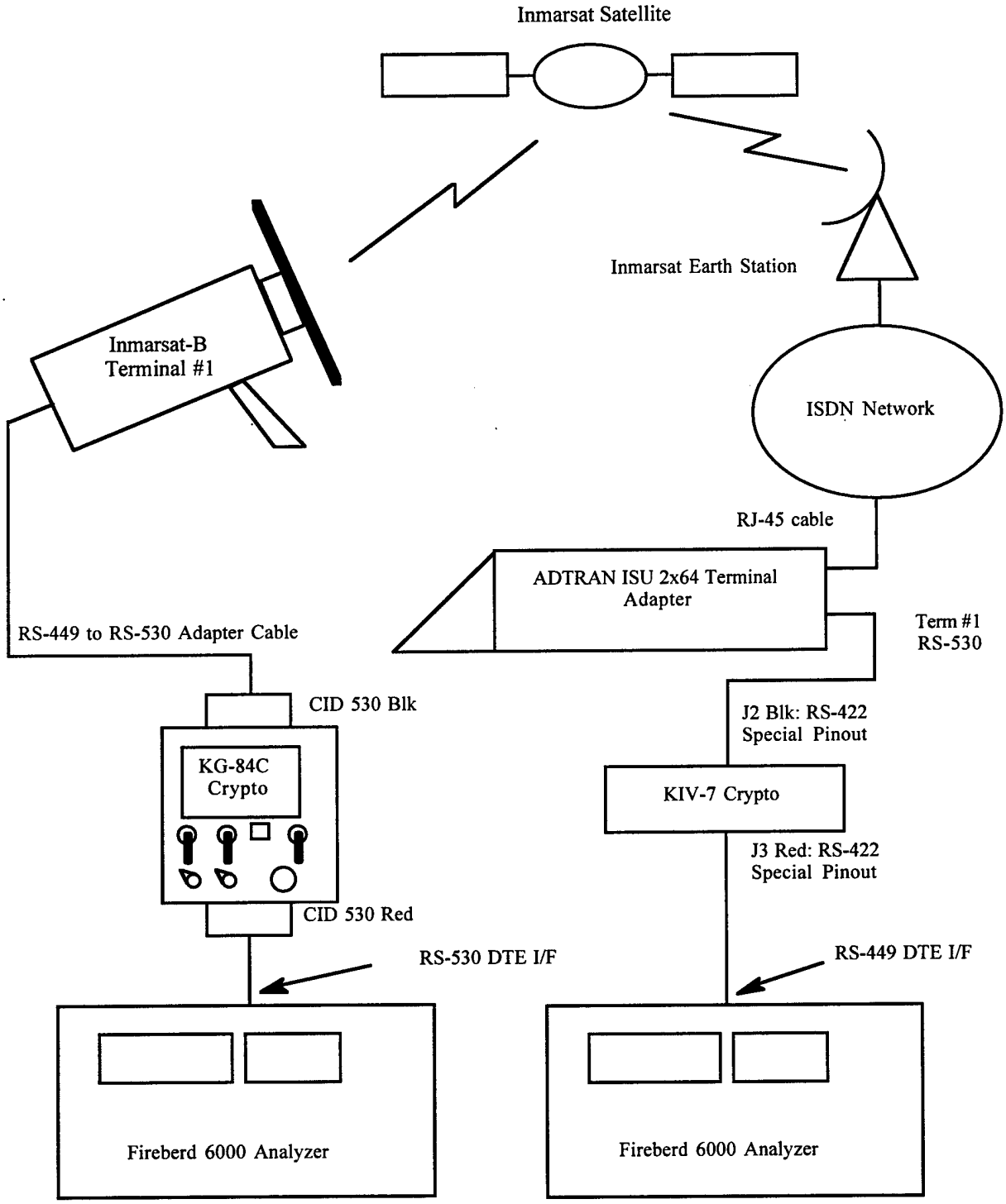

Figure 11
Inmarsat Compatibility Test with KG-84C and KIV-7 Cryptos

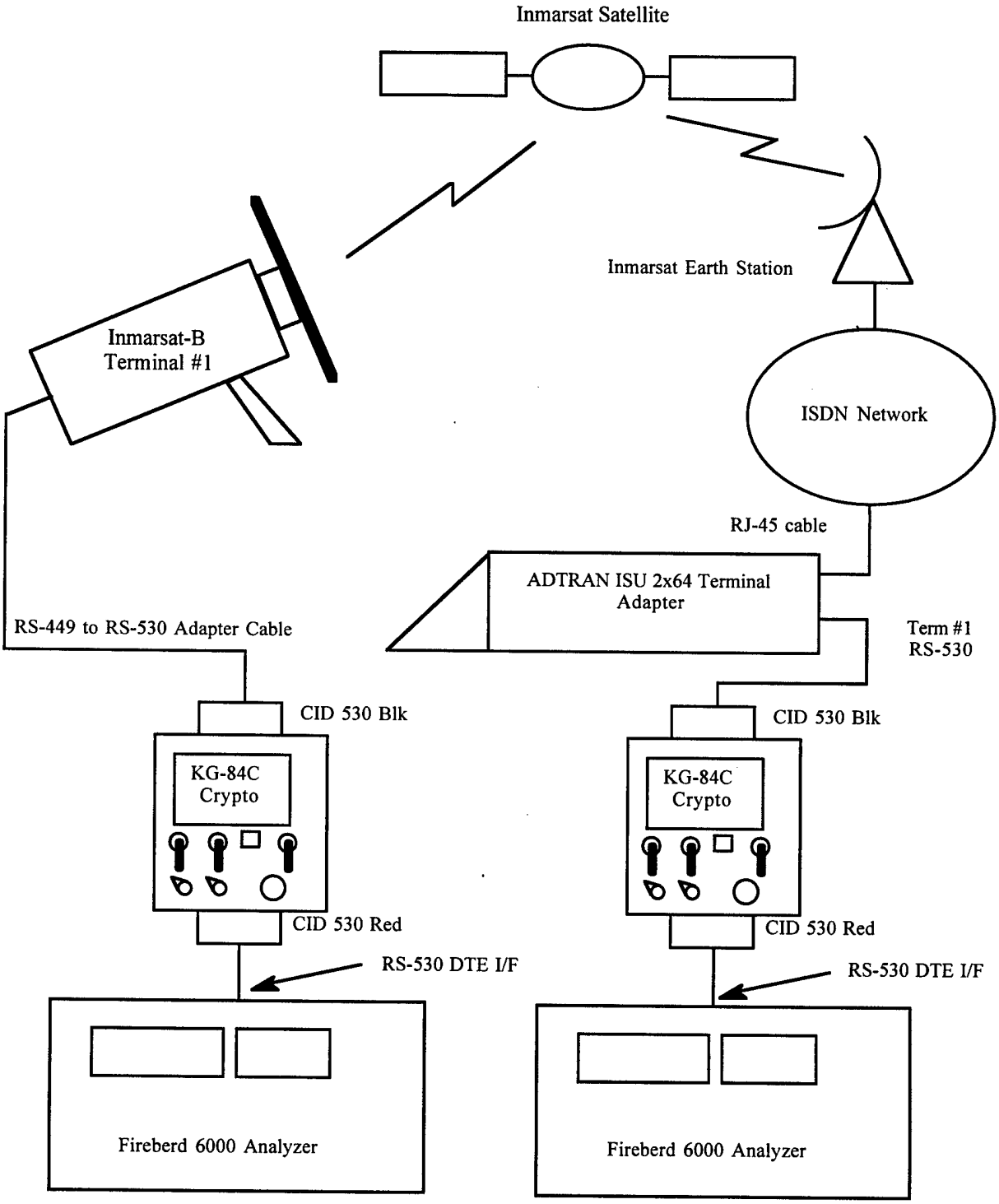

Figure 12
Inmarsat Compatibility Test with Two KG-84C Cryptos

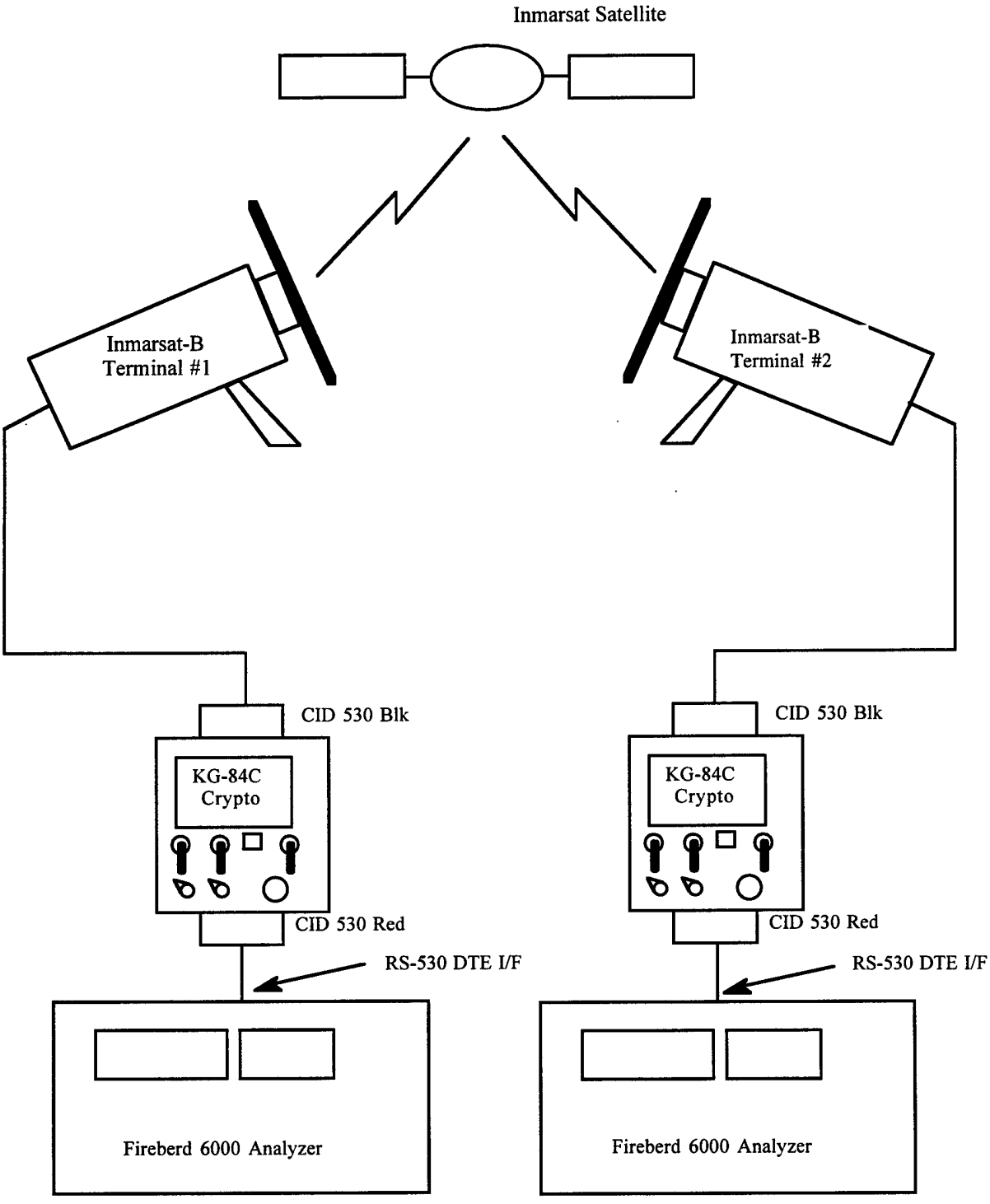

Figure 13
Inmarsat 64 kb/s Double-Hop Test with Two KG-84C Cryptos

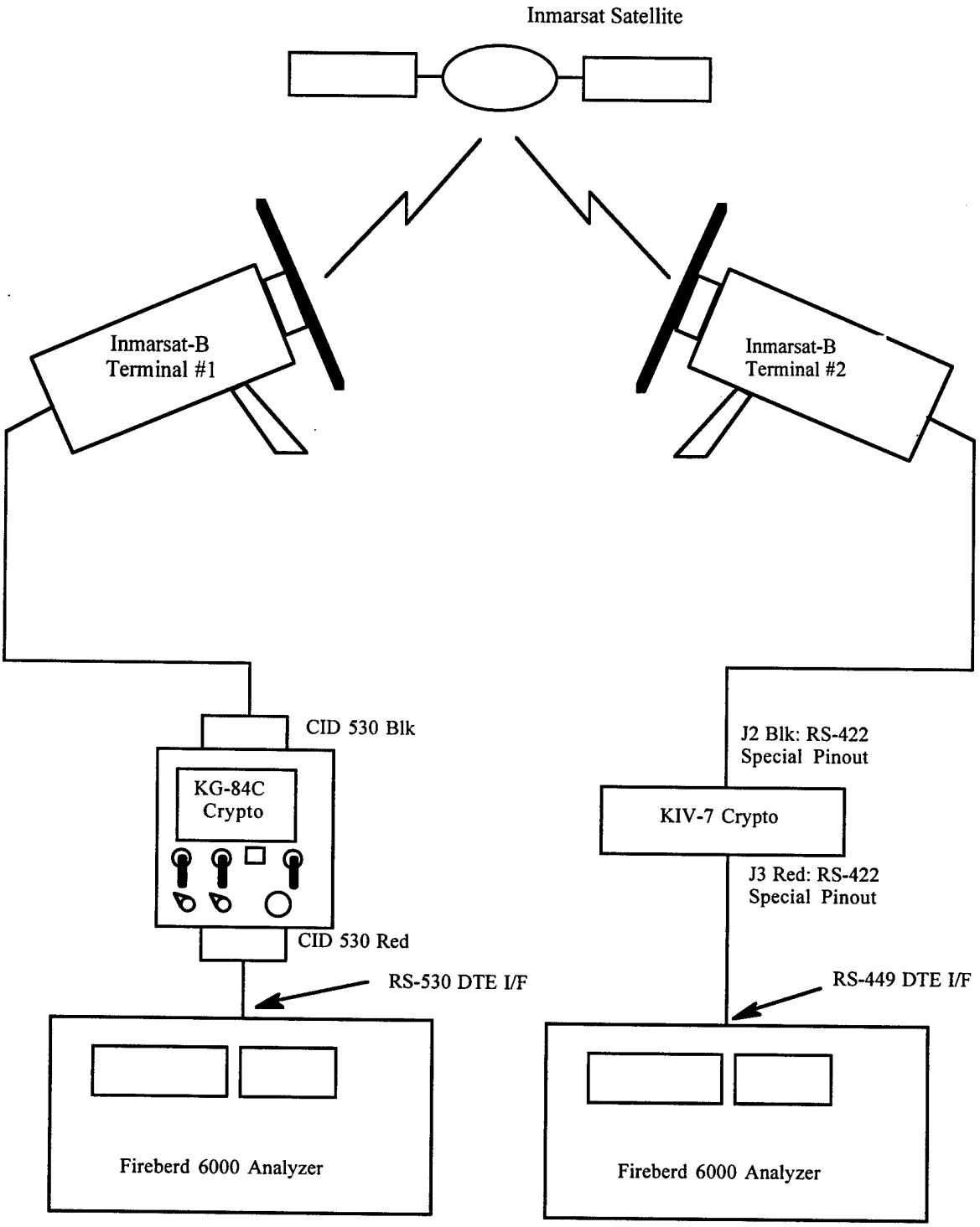

Figure 14
Inmarsat 64 kb/s Double-Hop Test with KG-84C and KIV-7 Cryptos

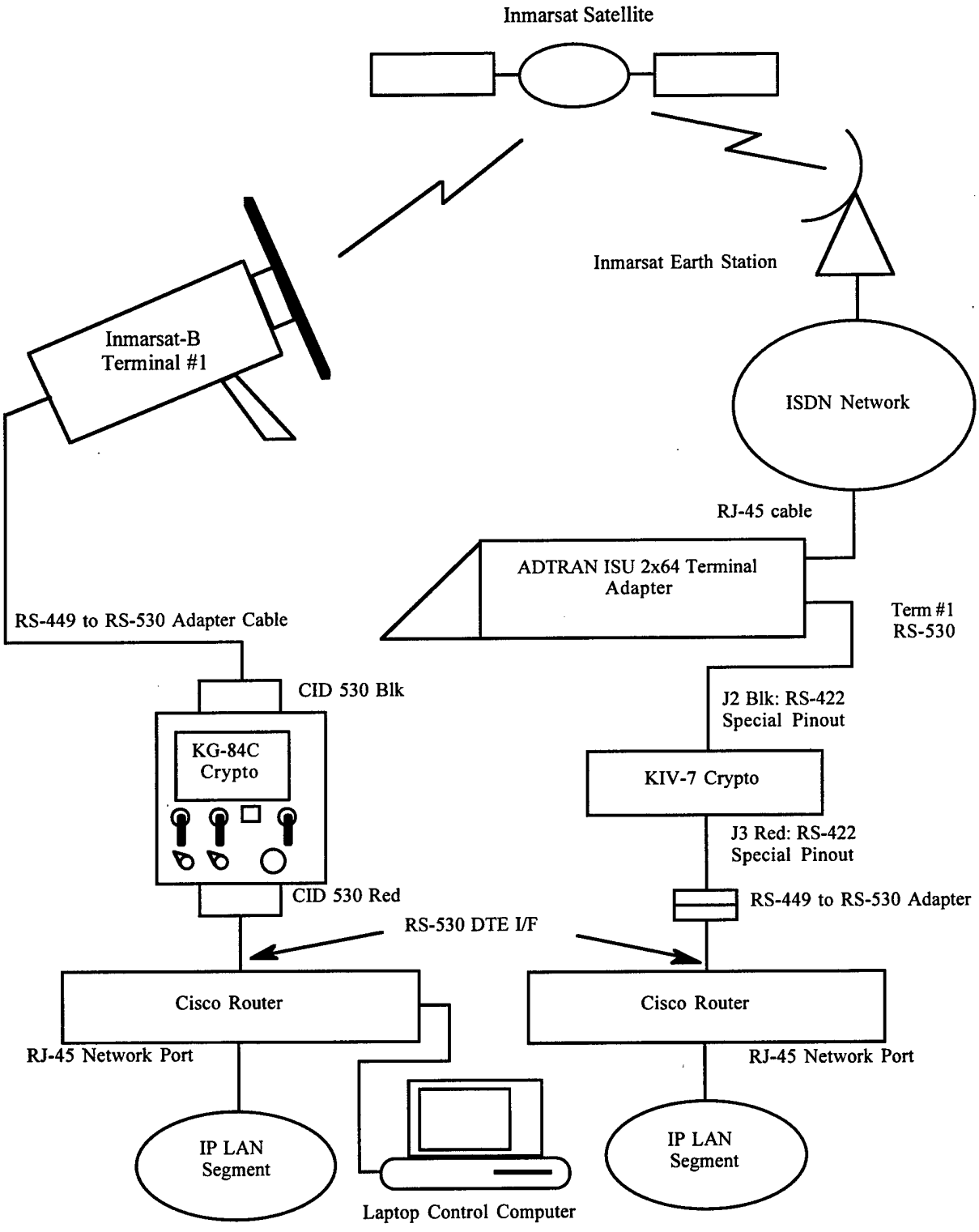

Figure 15
Inmarsat 64 kb/s Secure LAN Extension Test

APPENDIX B

TABLES

Table 1
Lynxx Terminal HSD Interface Notes

Device Type:	DCE
Electrical Interface:	RS-422
Pinout Spec.:	RS-449
Connector Type:	DB37F

Source	Signal name	Pin#	Comments	Pin#	Signal Name
	Frame ground/Shield	1			
		2		20	Receive Common
		3		21	
DTE	Send Data (A)	4		22	Send Data (B)
DCE	Transmit Timing (A)	5		23	Transmit Timing (B)
DCE	Receive Data (A)	6		24	Receive Data (B)
DTE	Request to Send (A)	7	Ignored by Lynxx	25	Request to Send (B)
DCE	Receive Timing (A)	8		26	Receive Timing (B)
DCE	Clear to Send (A)	9	Forced OFF by Lynxx	27	Clear to Send (B)
		10		28	
DCE	Data Mode (A)	11	Forced OFF by Lynxx	29	Data Mode (B)
DTE	Terminal Ready (A)	12	Sensed by Lynxx	30	Terminal Ready (B)
DCE	Receiver Ready (A)	13	Controlled by Lynxx	31	Receiver Ready (B)
		14		32	
		15		33	
		16		34	
DTE	Terminal Timing (A)	17	Ignored by Lynxx	35	Terminal Timing (B)
		18		36	
	Signal Ground	19		37	Send Common

Table 2

ADTRAN TA Setup Parameters for HSD Tests

Parameter Name	Parameter Setting Used	Addtional Param Setting
Configuration: Network - Dial Line		
Switch Protocol	National ISDN1	
Call Type: DTE1 & DTE2	Data 64 Kbps	
Terminal ID: DTE1	Set SPID=828124300	Set LDN=8281243
Terminal ID:DTE2	Set SPID=828210700	Set LDN=8282107
Busy Out	Enabled	
Dial Options	Front Panel	
Auto Answer	Enabled	
Answer Tone (DTE1 & DTE2)	Incoming Tone	
Connect Timeout	30 sec	
Call Screening	Answer Any	
SBUS Termination	100 Ohm On	
Configuration: DTE1 & DTE2 Options - Synchronous		
Bit Rate	64000.00	
Connector Type	RS-530	
RTS Options	1 ms Delay	
CTS Options	Forced CTS	
CD Options	Normal	
DTR Options	Ignore DTR	
DSR Options	DSR Forced On	
Transmit Clock	Normal	
Configuration: Protocol		
DTE1 & DTE2	Clear Channel	
Configuration: Quick Setup - Not Used		

Table 3

KIV-7 Setup Parameters for HSD Tests

Parameter Name	Parameter Setting Used	Description
Configuration Setup A		
Clk Sel	Master	Independent TX/Rx clocks.
SyncSel	RED, OP2	Redundant, OP2 robust sync mode
CommSel	FDX	Full duplex with end-around sync
DataMod	BB	Baseband data mode
DataLen	SYNCH/S	Synchronous/Synchronous Header Bypass mode
TX Rate	Ext DRC	External TX Data Rate Clock
RX Rate	Ext DRC	External RX Data Rate Clock
TTYmode	Auto	Automatic resynchroniztion
I/Fctrl	OFF	No interface control signal affected
Configuration Setup B		
Invert	none	Invert selected signals
TXClock	contTXC	Continuous transmit clock
RXClock	contRXC	Continuous receive clock
SyncOOS	Disabled	Synchronous Out-Of-Sync Detect Disabled
IdleSel	Disabled	Disabled, no added idles
AutoPhs	OFF	No Autophasing- wait for PTRS
UpdateU	Enabled	Automatic U-key Update Enabled
Configuration Setup C		
RED I/F	EIA-530	EIA-530 (RS-449) RED (Plaintext) interface
BLK I/F	EIA-530	EIA-530 (RS-449) BLACK (Ciphertext) interface
FIL I/F	102/Std	DS-102 (Common Fill), standard keys
FILaddr	254	DS-101 Fill Address Select
RCUaddr	31	Remote control address select
Display	Medium	Medium Intensity Display Brightness
Speaker	Enabled	Speaker Enabled

Table 4

RAD IMX-6L Inverse Multiplexer Configuration

Parameter Name	Parameter Setting Used	Addtional Param Setting
Command: DEF CALL P		
Call Profile # (P)	1	
CALL NAME	VIDEO128	
LOCAL_PORT	1	
REMOTE_PORT	1	
CALL_TYPE	BOND1	
BAND_BR	64	
PRF_BAND_M	2	
MIN_BAND_M	2	
CALL DESCRIPTION=	[blank]	
Command: DEF CALL P CHMAP		
Call Profile# (P)	1	
1	YES	
2	YES	
3 thru 6	NO	
Command: DEF CH X		
Channel Number (X)	1	ENABLED
	2	ENABLED
	3 thru 6	DISABLED
Command: DEF PORT [#]		
Port Number [#]	1	
BASE_RATE	x64	
MULT	2	
CLK_MODE	ST	
Command: DEF SYS		
CLK	EXT#1	
CALL1	1	
CALL2	--	

Table 5

CS8000 Multiplexer Setup Parameters for HSD Tests

Parameter Name	Parameter Setting Used
	Local (Master) & Remote (Slave) Config: Console Port
Rate	9.6K
Term	VT100
Alarm	Disable
	Local (Master) & Remote (Slave) Config: Data Ports
Port 2a (HP1645)	RS232 I/F,Internal clock,Online,Transp. signalling
Port 3a (FireBerd)	RS232 I/F,IBA clock,Online,Transparent signalling
Other Data Ports	Offline
	Local (Master) & Remote (Slave) Config: Mux Mode
Config 1	Voice port 6: manual rate 5.33 kbps
	Voice port 7: manual rate 32 kbps
	Data port 2a: sync,rate 2.4K
	Data port 3a: sync,rate 9.6K
	Local (Master) & Remote (Slave) Config: Network Port
Clock Mode	External
Clock Rate	64 kb/s
	Local (Master) Config: Voice Ports
Port 6 (STU III)	Echo Canc ENAB,IBA ENAB,Vocoder CELP ENAB,Online, Telco FXS LOOP_S
Port 7 (Handset)	Echo Canc ENAB,Vocoder CELP ENAB,Online, Telco FXS LOOP_S
	Remote (Slave) Config: Voice Ports
Port 6 (PSTN)	Echo Canc ENAB,IBA ENAB,Vocoder CELP ENAB,Online, Telco FXO
Port 7 (PSTN)	Echo Canc ENAB,Vocoder CELP ENAB,Online,Telco FXO

Table 6

KG-84C Setup Parameters for HSD Tests

Parameter Name	Parameter Setting Used	Description
Concealed Controls		
Clock	Master	Independent TX/Rx clocks.
Data Rate TX	EXT	External Tx Data Rate Clock
Data Rate RX	EXT	External Rx Data Rate Clock
TTY Mode	1 = AUTO	Automatic resynchroniztion
Data Length	SYNCH	Synchronous data
Sync Mode	5 = OP2	OP2 Robust Sync Mode
Comm Mode	1 = FDX	Full duplex with end-around sync
TDM	OFF	
Sync	OFF	
GRXC/CRXC	CRXC	Continuous RX Red side clocking
GTXC/CTXC	CTXC	Continuous TX Red side clocking
Internal Strapping		
PTRS Char Bypass	OUT	Red side RTS not bypassed
Time	5 Sec	5 second time out
IDLS	OUT	Disabled, no added idles
KEX (VU)	OUT	Disabled
COND	OUT	Unconditioned Baseband Data

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence Research Establishment Ottawa
Ottawa, Ontario
K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

DREO Secure Video Conferencing and High Speed Data Encryption Tests for Inmarsat-B Satellite Terminals (U)

4. AUTHORS (Last name, first name, middle initial)

Lambert, James D.

5. DATE OF PUBLICATION (month and year of publication of document)

October 1999

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

50

6b. NO. OF REFS (total cited in document)

10

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

DREO Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

National Defence, Directorate of Telecommunications and Spectrum Engineering Services
219 Laurier Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DREO TM 1999-084

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

UNCLASSIFIED
SECURITY CLASSIFICATION OF FORM

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

The aim of this report is to describe the results of a series of tests performed between 1996 and 1999 using Inmarsat-B satellite terminals. These tests were designed to evaluate the use of Commercial-Off-The-Shelf (COTS) equipment in demonstrating low-rate, secure video conferencing, multiplexed voice and data circuits, and LAN extension services via the Inmarsat-B 64 kb/s High Speed Data (HSD) service. Successful demonstrations of both secure point-to-point, and secure remote-to-Defence Video Conferencing Network (DVCN) were conducted.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Inmarsat-B
High Speed Data
HSD
Video Conferencing
Secure Video Conferencing
Secure LAN Extension
Satellite Terminal
Mobile Satellite Terminal